



## **Cisco IOS Multiprotocol Label Switching Configuration Guide**

Release 12.2SR

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883

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

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

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

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

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

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

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

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

*Cisco IOS Multiprotocol Label Switching Configuration Guide*  
© 2010 Cisco Systems, Inc. All rights reserved.



# Using the Command-Line Interface in Cisco IOS Software

---

**Last Updated: October 14, 2009**

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

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

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

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

## Initially Configuring a Device

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

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

### Changing the Default Settings for a Console or AUX Port

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

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

**Note**

The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

## Using the CLI

This section describes the following topics:

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

## Understanding Command Modes

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

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



**Table 1**     *CLI Command Modes*

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

**Table 1** CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
ROM monitor	From privileged EXEC mode, issue the <b>reload</b> command. Press the <b>Break</b> key during the first 60 seconds while the system is booting.	rommon # >  The # symbol represents the line number and increments at each prompt.	Issue the <b>continue</b> command.	<ul style="list-style-type: none"> <li>Run as the default operating mode when a valid image cannot be loaded.</li> <li>Access the fall-back procedure for loading an image when the device lacks a valid image and cannot be booted.</li> <li>Perform password recovery when a Ctrl-Break sequence is issued within 60 seconds of a power-on or reload event.</li> </ul>
Diagnostic (available only on Cisco ASR 1000 series routers)	<p>The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload.</p> <ul style="list-style-type: none"> <li>A user-configured access policy was configured using the <b>transport-map</b> command, which directed the user into diagnostic mode.</li> <li>The router was accessed using an RP auxiliary port.</li> <li>A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.</li> </ul>	Router(diag)#	<p>If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI.</p> <p>If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.</p>	<ul style="list-style-type: none"> <li>Inspect various states on the router, including the Cisco IOS state.</li> <li>Replace or roll back the configuration.</li> <li>Provide methods of restarting the Cisco IOS software or other processes.</li> <li>Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components.</li> <li>Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.</li> </ul>

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

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

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

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

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



**Note**

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

## Using the Interactive Help Feature

The CLI includes an interactive Help feature. [Table 2](#) describes the purpose of the CLI interactive Help commands.

**Table 2** CLI Interactive Help Commands

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

The following examples show how to use the help commands:

### **help**

```
Router> help
```

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

Two styles of help are provided:

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

### **?**

```
Router# ?
```

```
Exec commands:
```

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

```
<snip>
```

### **partial command?**

```
Router(config)# zo?
```

```
zone zone-pair
```

### **partial command<Tab>**

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

### **command ?**

```
Router(config-if)# pppoe ?
```

enable	Enable pppoe
max-sessions	Maximum PPPOE sessions

### **command keyword ?**

```
Router(config-if)# pppoe enable ?
```

group	attach a BBA group
-------	--------------------

```
<cr>
```

## Understanding Command Syntax

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

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

**Table 3**     *CLI Syntax Conventions*

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

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
WORD domain name
Router(config)# ethernet cfm domain dname ?
level
Router(config)# ethernet cfm domain dname level ?
<0-7> maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
<cr>

Router(config)# snmp-server file-transfer access-group 10 ?
protocol protocol options
<cr>

Router(config)# logging host ?
Hostname or A.B.C.D IP address of the syslog server
ipv6 Configure IPv6 syslog server
```

## Understanding Enable and Enable Secret Passwords

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

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

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

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

**Note**

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

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

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

For more information about password recovery procedures for Cisco products, see [http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products\\_tech\\_note09186a00801746e6.shtml](http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml).

## Using the Command History Feature

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

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

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

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

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

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

- Press Ctrl-P or the Up Arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the Down Arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

**Note**

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

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

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

## Abbreviating Commands

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

## Using Aliases for CLI Commands

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

Table 4 shows the default command aliases.

**Table 4**     *Default Command Aliases*

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

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

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

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

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

[http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf\\_a1.html](http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.html).

## Using the no and default Forms of Commands

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

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

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

## Using the debug Command

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

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at [http://www.cisco.com/en/US/docs/ios/debug/command/reference/db\\_book.html](http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html).



### Caution

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

## Filtering Output Using Output Modifiers

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

The following three output modifiers are available:

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

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



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

```
Router# show interface | include protocol

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

## Understanding CLI Error Messages

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

**Table 5** Common CLI Error Messages

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

For more system error messages, see the following document:

- [Cisco IOS Release 12.4T System Message Guide](#)

## Saving Changes to a Configuration

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

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

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

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

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

## Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*  
[http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf\\_cli-basics.html](http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html)
- Cisco Product/Technology Support  
<http://www.cisco.com/go/techdocs>
- Support area on Cisco.com (also search for documentation by task or product)  
<http://www.cisco.com/en/US/support/index.html>
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com user ID and password)  
<http://www.cisco.com/kobayashi/sw-center/>
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software  
<http://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com user ID and password)  
<http://tools.cisco.com/Support/CLILookup>
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands  
<http://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>

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

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

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

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



# About Cisco IOS Software Documentation

---

**Last Updated: November 20, 2009**

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

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

## Documentation Objectives

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

## Audience

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

## Documentation Conventions

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

This section contains the following topics:

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

## Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

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

## Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
<b>bold</b>	Bold text indicates commands and keywords that you enter as shown.
<i>italic</i>	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, that is enclosed within braces or square brackets indicates a choice within a set of keywords or arguments.
[x   y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x   y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y   z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

## Software Conventions

Cisco IOS software uses the following program code conventions:

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

## Reader Alert Conventions

Cisco IOS documentation uses the following conventions for reader alerts:



### Caution

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



### Note

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



### Timesaver

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

## Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

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

# Cisco IOS Documentation Set

The Cisco IOS documentation set consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Command pages are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

## Cisco IOS Documentation on Cisco.com

The following sections describe the organization of the Cisco IOS documentation set and how to access various document types.

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

### New Features List

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

### Feature Guides

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

### Configuration Guides

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

### Command References

Command reference books contain descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

### Cisco IOS Supplementary Documents and Resources

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

## Configuration Guides, Command References, and Supplementary Resources

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

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

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

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

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"><li>• <i>Cisco IOS AppleTalk Configuration Guide</i></li><li>• <i>Cisco IOS AppleTalk Command Reference</i></li></ul>	AppleTalk protocol.
<ul style="list-style-type: none"><li>• <i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i></li><li>• <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i></li></ul>	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></li> <li><i>Cisco IOS Bridging Command Reference</i></li> <li><i>Cisco IOS IBM Networking Command Reference</i></li> </ul>	<p>Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM).</p> <p>Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.</p>
<ul style="list-style-type: none"> <li><i>Cisco IOS Broadband Access Aggregation and DSL Configuration Guide</i></li> <li><i>Cisco IOS Broadband Access Aggregation and DSL Command Reference</i></li> </ul>	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).
<ul style="list-style-type: none"> <li><i>Cisco IOS Carrier Ethernet Configuration Guide</i></li> <li><i>Cisco IOS Carrier Ethernet Command Reference</i></li> </ul>	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and Operation, Administration, and Maintenance (OAM).
<ul style="list-style-type: none"> <li><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></li> <li><i>Cisco IOS Configuration Fundamentals Command Reference</i></li> </ul>	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.
<ul style="list-style-type: none"> <li><i>Cisco IOS DECnet Configuration Guide</i></li> <li><i>Cisco IOS DECnet Command Reference</i></li> </ul>	DECnet protocol.
<ul style="list-style-type: none"> <li><i>Cisco IOS Dial Technologies Configuration Guide</i></li> <li><i>Cisco IOS Dial Technologies Command Reference</i></li> </ul>	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
<ul style="list-style-type: none"> <li><i>Cisco IOS Flexible NetFlow Configuration Guide</i></li> <li><i>Cisco IOS Flexible NetFlow Command Reference</i></li> </ul>	Flexible NetFlow.
<ul style="list-style-type: none"> <li><i>Cisco IOS High Availability Configuration Guide</i></li> <li><i>Cisco IOS High Availability Command Reference</i></li> </ul>	A variety of high availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
<ul style="list-style-type: none"> <li><i>Cisco IOS Integrated Session Border Controller Command Reference</i></li> </ul>	A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS).



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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li><i>Cisco IOS Intelligent Services Gateway Configuration Guide</i></li> <li><i>Cisco IOS Intelligent Services Gateway Command Reference</i></li> </ul>	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and session state monitoring.
<ul style="list-style-type: none"> <li><i>Cisco IOS Interface and Hardware Component Configuration Guide</i></li> <li><i>Cisco IOS Interface and Hardware Component Command Reference</i></li> </ul>	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Addressing Services Configuration Guide</i></li> <li><i>Cisco IOS IP Addressing Services Command Reference</i></li> </ul>	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Application Services Configuration Guide</i></li> <li><i>Cisco IOS IP Application Services Command Reference</i></li> </ul>	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Mobility Configuration Guide</i></li> <li><i>Cisco IOS IP Mobility Command Reference</i></li> </ul>	Mobile ad hoc networks (MANet) and Cisco mobile networks.
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Multicast Configuration Guide</i></li> <li><i>Cisco IOS IP Multicast Command Reference</i></li> </ul>	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: BFD Configuration Guide</i></li> </ul>	Bidirectional forwarding detection (BFD).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: BGP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: BGP Command Reference</i></li> </ul>	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: EIGRP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: EIGRP Command Reference</i></li> </ul>	Enhanced Interior Gateway Routing Protocol (EIGRP).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: ISIS Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: ISIS Command Reference</i></li> </ul>	Intermediate System-to-Intermediate System (IS-IS).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: ODR Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: ODR Command Reference</i></li> </ul>	On-Demand Routing (ODR).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: OSPF Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: OSPF Command Reference</i></li> </ul>	Open Shortest Path First (OSPF).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: Protocol-Independent Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: Protocol-Independent Command Reference</i></li> </ul>	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Routing: RIP Configuration Guide</i></li> <li><i>Cisco IOS IP Routing: RIP Command Reference</i></li> </ul>	Routing Information Protocol (RIP).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP SLAs Configuration Guide</i></li> <li><i>Cisco IOS IP SLAs Command Reference</i></li> </ul>	Cisco IOS IP Service Level Agreements (IP SLAs).
<ul style="list-style-type: none"> <li><i>Cisco IOS IP Switching Configuration Guide</i></li> <li><i>Cisco IOS IP Switching Command Reference</i></li> </ul>	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
<ul style="list-style-type: none"> <li><i>Cisco IOS IPv6 Configuration Guide</i></li> <li><i>Cisco IOS IPv6 Command Reference</i></li> </ul>	For IPv6 features, protocols, and technologies, go to the IPv6 <a href="#">“Start Here”</a> document.
<ul style="list-style-type: none"> <li><i>Cisco IOS ISO CLNS Configuration Guide</i></li> <li><i>Cisco IOS ISO CLNS Command Reference</i></li> </ul>	ISO Connectionless Network Service (CLNS).
<ul style="list-style-type: none"> <li><i>Cisco IOS LAN Switching Configuration Guide</i></li> <li><i>Cisco IOS LAN Switching Command Reference</i></li> </ul>	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i></li> </ul>	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Home Agent Command Reference</i></li> </ul>	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i></li> </ul>	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
<ul style="list-style-type: none"> <li><i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i></li> <li><i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i></li> </ul>	Cisco IOS radio access network products.
<ul style="list-style-type: none"> <li><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></li> <li><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></li> </ul>	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS traffic engineering (TE), and MPLS Embedded Management (EM) and MIBs.
<ul style="list-style-type: none"> <li><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></li> <li><i>Cisco IOS Multi-Topology Routing Command Reference</i></li> </ul>	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
<ul style="list-style-type: none"> <li><i>Cisco IOS NetFlow Configuration Guide</i></li> <li><i>Cisco IOS NetFlow Command Reference</i></li> </ul>	Network traffic data analysis, aggregation caches, and export features.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Network Management Configuration Guide</i></li> <li>• <i>Cisco IOS Network Management Command Reference</i></li> </ul>	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS software (XSM Configuration).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Novell IPX Configuration Guide</i></li> <li>• <i>Cisco IOS Novell IPX Command Reference</i></li> </ul>	Novell Internetwork Packet Exchange (IPX) protocol.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Optimized Edge Routing Configuration Guide</i></li> <li>• <i>Cisco IOS Optimized Edge Routing Command Reference</i></li> </ul>	Optimized edge routing (OER) monitoring; Performance Routing (PfR); and automatic route optimization and load distribution for multiple connections between networks.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Quality of Service Solutions Configuration Guide</i></li> <li>• <i>Cisco IOS Quality of Service Solutions Command Reference</i></li> </ul>	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Command Reference</i></li> </ul>	Access control lists (ACLs); authentication, authorization, and accounting (AAA); firewalls; IP security and encryption; neighbor router authentication; network access security; network data encryption with router authentication; public key infrastructure (PKI); RADIUS; TACACS+; terminal access security; and traffic filters.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing the Data Plane</i></li> </ul>	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i></li> </ul>	Control Plane Policing, Neighborhood Router Authentication.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Securing User Services</i></li> </ul>	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Security Configuration Guide: Secure Connectivity</i></li> </ul>	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Service Advertisement Framework Configuration Guide</i></li> <li>• <i>Cisco IOS Service Advertisement Framework Command Reference</i></li> </ul>	Cisco Service Advertisement Framework.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Service Selection Gateway Configuration Guide</i></li> <li>• <i>Cisco IOS Service Selection Gateway Command Reference</i></li> </ul>	Subscriber authentication, service access, and accounting.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Activation Configuration Guide</i></li> <li>• <i>Cisco IOS Software Activation Command Reference</i></li> </ul>	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Software Modularity Installation and Configuration Guide</i></li> <li>• <i>Cisco IOS Software Modularity Command Reference</i></li> </ul>	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes, and patches.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Terminal Services Configuration Guide</i></li> <li>• <i>Cisco IOS Terminal Services Command Reference</i></li> </ul>	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Virtual Switch Command Reference</i></li> </ul>	<p>Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).</p> <p><b>Note</b> For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.</p>
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Voice Configuration Library</i></li> <li>• <i>Cisco IOS Voice Command Reference</i></li> </ul>	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS VPDN Configuration Guide</i></li> <li>• <i>Cisco IOS VPDN Command Reference</i></li> </ul>	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy; L2TP extended failover; L2TP security VPDN; multihop by Dialed Number Identification Service (DNIS); timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F); RADIUS Attribute 82 (tunnel assignment ID); shell-based authentication of VPDN users; tunnel authentication via RADIUS on tunnel terminator.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wide-Area Networking Configuration Guide</i></li> <li>• <i>Cisco IOS Wide-Area Networking Command Reference</i></li> </ul>	Frame Relay; Layer 2 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); and X.25.
<ul style="list-style-type: none"> <li>• <i>Cisco IOS Wireless LAN Configuration Guide</i></li> <li>• <i>Cisco IOS Wireless LAN Command Reference</i></li> </ul>	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

**Table 2** Cisco IOS Supplementary Documents and Resources

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

## Additional Resources and Documentation Feedback

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

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

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

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

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

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

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



## **Basic MPLS**







# MPLS Static Labels

---

**First Published: October 2002**

**Last Updated: July 13, 2007**

This document describes the Cisco MPLS Static Labels feature. It identifies the supported platforms, provides configuration examples, and lists related Cisco IOS command-line interface (CLI) commands.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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

## **History for the MPLS Static Labels feature**

<b>Release</b>	<b>Modification</b>
12.0(23)S	This feature was introduced.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.

## Contents

- [Feature Overview, page 2](#)
- [Prerequisites, page 2](#)
- [Configuration Tasks, page 3](#)
- [Monitoring and Maintaining MPLS Static Labels, page 4](#)
- [Configuration Examples, page 5](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Glossary, page 9](#)



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Feature Overview

Generally, label switching routers (LSRs) dynamically learn the labels they should use to label-switch packets by means of label distribution protocols that include:

- Label Distribution Protocol (LDP), the Internet Engineering Task Force (IETF) standard, used to bind labels to network addresses
- Resource Reservation Protocol (RSVP) used to distribute labels for traffic engineering (TE)
- Border Gateway Protocol (BGP) used to distribute labels for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs)

To use a learned label to label-switch packets, an LSR installs the label into its Label Forwarding Information Base (LFIB).

The MPLS Static Labels feature provides the means to configure statically:

- The binding between a label and an IPv4 prefix
- The contents of an LFIB crossconnect entry

## Benefits

### Static Bindings Between Labels and IPv4 Prefixes

Static bindings between labels and IPv4 prefixes can be configured to support MPLS hop-by-hop forwarding through neighbor routers that do not implement LDP label distribution.

### Static Crossconnects

Static crossconnects can be configured to support MPLS Label Switched Path (LSP) midpoints when neighbor routers do not implement either the LDP or RSVP label distribution, but do implement an MPLS forwarding path.

## Restrictions

- The trouble shooting process for MPLS static labels is complex.
- On a provider edge (PE) router for MPLS VPNs, there is no mechanism for statically binding a label to a customer network prefix (VPN IPv4 prefix).
- MPLS static crossconnect labels remain in the LFIB even if the router to which the entry points goes down.
- MPLS static crossconnect mappings remain in effect even with topology changes.
- MPLS static labels are not supported for label-controlled Asynchronous Transfer Mode (lc-atm).
- MPLS static bindings are not supported for local prefixes.

## Prerequisites

The network must support the following Cisco IOS features before you enable MPLS static labels:

- Multiprotocol Label Switching (MPLS)
- IP Cisco Express Forwarding

# Configuration Tasks

See the following sections for the configuration tasks for the this feature:

- [Configuring MPLS Static Prefix/Label Bindings, page 3](#) (required)
- [Verifying MPLS Static Prefix/Label Bindings, page 3](#) (optional)
- [Configuring MPLS Static Crossconnects, page 4](#) (required)
- [Verifying MPLS Static Crossconnect Configuration, page 4](#) (optional)

## Configuring MPLS Static Prefix/Label Bindings

To configure MPLS static prefix/label bindings, use the following commands beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>mpls label range</b> <i>min-label max-label [static</i> <i>min-static-label max-static-label]</i>	Specifies a range of labels for use with MPLS Static Labels feature.  (Default is no labels reserved for static assignment.)
<b>Step 3</b>	Router(config)# <b>mpls static binding ipv4</b> <i>prefix mask [input   output nexthop]</i> <i>label</i>	Specifies static binding of labels to IPv4 prefixes.  Bindings specified are installed automatically in the MPLS forwarding table as routing demands.

## Verifying MPLS Static Prefix/Label Bindings

To verify the configuration for MPLS static prefix/label bindings, use this procedure:

- Step 1** Enter **show mpls label range** command. The output shows that the new label ranges do not take effect until a reload occurs:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 16/100000
    [Configured range for next reload: Min/Max label: 200/100000]
Range for static labels: Min/Max/Number: 16/199
```

The following output from the **show mpls label range** command, executed after a reload, indicates that the new label ranges are in effect:

```
Router# show mpls label range

Downstream label pool: Min/Max label: 200/100000
Range for static labels: Min/Max/Number: 16/199
```

- Step 2** Enter the **show mpls static binding ipv4** command to show the configured static prefix/label bindings:

```
Router# show mpls static binding ipv4

10.17.17.17/32: Incoming label: 251 (in LIB)
```

```

    Outgoing labels:
      10.0.0.1          18
10.18.18.18/32: Incoming label: 201 (in LIB)
    Outgoing labels:
10.0.0.1implicit-null

```

- Step 3** Use the **show mpls forwarding-table** command to determine which static prefix/label bindings are currently in use for MPLS forwarding.

```
Router# show mpls forwarding-table
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
201	Pop tag	10.18.18.18/32	0	PO1/1/0	point2point
	2/35	10.18.18.18/32	0	AT4/1/0.1	point2point
251	18	10.17.17.17/32	0	PO1/1/0	point2point

## Configuring MPLS Static Crossconnects

To configure MPLS static crossconnects, use the following command beginning in global configuration mode:

	Command	Purpose
<b>Step 1</b>	Router# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 2</b>	Router(config)# <b>mpls label range</b> <i>min-label max-label [static</i> <i>min-static-label max-static-label]</i>	Specifies a range of labels for use with MPLS Static Labels feature.  (Default is no labels reserved for static assignment.)
<b>Step 3</b>	Router(config)# <b>mpls static binding ipv4</b> <i>prefix mask [input   output nexthop]</i> <i>label</i>	Specifies static binding of labels to IPv4 prefixes.  Bindings specified are installed automatically in the MPLS forwarding table as routing demands.

## Verifying MPLS Static Crossconnect Configuration

To verify the configuration for MPLS static crossconnects, use this procedure:

- Step 1** Use the **show mpls static crossconnect** command to display information about crossconnects that have been configured:

```
Router# show mpls static crossconnect
```

Local label	Outgoing label	Outgoing interface	Next Hop
34	22	pos3/0	point2point (in LFIB)

## Monitoring and Maintaining MPLS Static Labels

Refer to the following Table to monitor and maintain MPLS Static Labels.

Command	Purpose
Router# <b>show mpls forwarding-table</b>	Displays the contents of the MPLS LFIB.
Router# <b>show mpls label range</b>	Displays information about the static label range.
Router# <b>show mpls static binding ipv4</b>	Displays information about the configured static prefix/label bindings.
Router# <b>show mpls static crossconnect</b>	Displays information about the configured crossconnects.

## Configuration Examples

This section provides the following configuration examples for the MPLS Static Labels feature:

- [Configuring MPLS Static Prefixes/Labels Example, page 5](#)
- [Configuring MPLS Static Crossconnects Example, page 6](#)

### Configuring MPLS Static Prefixes/Labels Example

In the following output, the **mpls label range** command reconfigures the range used for dynamically assigned labels from 16 to 100000 to 200 to 100000 and configures a static label range of 16 to 199.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# mpls label range 200 100000 static 16 199
```

```
% Label range changes take effect at the next reload.
```

```
Router(config)# end
```

In the following output, the **show mpls label range** command indicates that the new label ranges do not take effect until a reload occurs:

```
Router# show mpls label range
```

```
Downstream label pool: Min/Max label: 16/100000  
[Configured range for next reload: Min/Max label: 200/100000]  
Range for static labels: Min/Max/Number: 16/199
```

In the following output, the **show mpls label range** command, executed after a reload, indicates that the new label ranges are in effect:

```
Router# show mpls label range
```

```
Downstream label pool: Min/Max label: 200/100000  
Range for static labels: Min/Max/Number: 16/199
```

In the following output, the **mpls static binding ipv4** commands configure static prefix/label bindings. They also configure input (local) and output (remote) labels for various prefixes:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 55
```

```

Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.0.0.66 2607

Router(config)# mpls static binding ipv4 10.6.0.0 255.255.0.0 input 17

Router(config)# mpls static binding ipv4 10.0.0.0 255.0.0.0 output 10.13.0.8 explicit-null

Router(config)# end

```

In the following output, the **show mpls static binding ipv4** command displays the configured static prefix/label bindings:

```

Router# show mpls static binding ipv4

10.0.0.0/8: Incoming label: none;
    Outgoing labels:
10.13.0.8          explicit-null
10.0.0.0/8: Incoming label: 55 (in LIB)
    Outgoing labels:
    10.0.0.66          2607
10.66.0.0/16: Incoming label: 17 (in LIB)
    Outgoing labels:  None

```

## Configuring MPLS Static Crossconnects Example

In the following output, the **mpls static crossconnect** command configures a crossconnect from incoming label 34 to outgoing label 22 out interface pos3/0:

```

Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# mpls static crossconnect 34 pos3/0 22

Router(config)# end

```

In the following output, the **show mpls static crossconnect** command displays the configured crossconnect:

```

Router# show mpls static crossconnect

Local  Outgoing  Outgoing  Next Hop
label  label     interface
34     22        pos3/0    point2point (in LFIB)

```

## Additional References

The following sections provide references related to the MPLS Static Labels feature.

## Related Documents

Related Topic	Document Title
MPLS commands	<a href="#">Multiprotocol Label Switching Command Reference</a>

## Standards

Standard	Title
None	—

## MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
None	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls static binding**
- **mpls label range**
- **mpls static binding ipv4**
- **mpls static crossconnect**
- **show mpls label range**
- **show mpls static binding ipv4**
- **show mpls static crossconnect**



# Glossary

**BGP**—Border Gateway Protocol. The predominant interdomain routing protocol used in IP networks.

**Border Gateway Protocol**—See BGP.

**FIB**—Forwarding Information Base. A table that contains a copy of the forwarding information in the IP routing table.

**Forwarding Information Base**—See FIB.

**label**—A short, fixed-length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

**label binding**—An association between a label and a set of packets, which can be advertised to neighbors so that a label switched path can be established.

**Label Distribution Protocol**—See LDP.

**Label Forwarding Information Base**—See LFIB.

**label imposition**—The act of putting the first label on a packet.

**label switching router**—See LSR.

**LDP**—Label Distribution Protocol. The protocol that supports MPLS hop-by-hop forwarding by distributing bindings between labels and network prefixes.

**LFIB**—Label Forwarding Information Base. A data structure in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSR**—label switching router. A Layer 3 router that forwards a packet based on the value of an identifier encapsulated in the packet.

**MPLS**—Multiprotocol Label Switching. An industry standard on which label switching is based.

**MPLS hop-by-hop forwarding**—The forwarding of packets along normally routed paths using MPLS forwarding mechanisms.

**Multiprotocol Label Switching**—See MPLS.

**Resource Reservation Protocol**—See RSVP.

**RIB**—Routing Information Base. A common database containing all the routing protocols running on a router.

**Routing Information Base**—See RIB.

**RSVP**—Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

**traffic engineering**—Techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**Virtual Private Network**—See VPN.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



# NetFlow MPLS Label Export

---

**First Published: February 23, 2006**

**Last Updated: February 15, 2008**

The NetFlow MPLS Label Export feature allows a label switch router (LSR) to collect and export Multiprotocol Label Switching (MPLS) labels allocated by the LSR when an adjacent router pushes that label on the top of the label stack of a transit packet. At the same time, the LSR collects the prefix associated with the MPLS label and the application that allocated the label. The router collects the information in a table called the MPLS Prefix/Application/Label (PAL) table and exports this data to a NetFlow collector as the label is allocated or, if so configured, periodically exports the full MPLS PAL table.

You can use this information to create a provider edge (PE)-to-PE matrix, which is useful for network traffic planning and billing. To realize this benefit, you must export the MPLS label information to a NetFlow collector for analysis. This feature also provides information that a NetFlow collector can use to create a Virtual Private Network (VPN) routing and forwarding instance (VRF)-to-PE and PE-to-VRF matrix.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for NetFlow MPLS Label Export”](#) section on page 16.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

## Contents

- [Prerequisites for NetFlow MPLS Label Export, page 2](#)
- [Restrictions for NetFlow MPLS Label Export, page 2](#)
- [Information About NetFlow MPLS Label Export, page 3](#)



---

**Americas Headquarters:**

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.

- [How to Configure NetFlow MPLS Label Export, page 7](#)
- [Configuration Examples for NetFlow MPLS Label Export, page 12](#)
- [Additional References, page 13](#)
- [Command Reference, page 15](#)
- [Feature Information for NetFlow MPLS Label Export, page 16](#)
- [Glossary, page 17](#)

## Prerequisites for NetFlow MPLS Label Export

The NetFlow MPLS Label Export feature requires the following:

- NetFlow configured on the LSR
- MPLS enabled on the LSR

If you are exporting data to a Cisco NetFlow collector, the following requirements apply:

- NetFlow Version 9 export format configured on the LSR
- NetFlow collector and analyzer that can use MPLS PAL records exported in NetFlow Version 9 format

## Restrictions for NetFlow MPLS Label Export

The following restrictions apply to the NetFlow MPLS Label Export feature for Cisco IOS 12.2S releases and Cisco IOS Release 12.5(1):

- The MPLS PAL table does not support the export of information for the following:
  - IP Version 6 (IPv6) labels
  - IP Multicast labels
  - Quality of service (QoS) labels
  - Traffic engineering (TE) tunnel headend labels
- The ability to create a VRF-to-VRF traffic matrix is not supported.
- If one application deallocates a label and a second application soon reallocates the same label, the NetFlow collector might not be able to determine how many packets flowed while the label was owned by each application.
- In MPLS PAL table records, for labels allocated by VPNs, Border Gateway Protocol (BGP) IPv4, or BGP VPN Version 4 (VPNv4), the stored prefix can be either 0.0.0.0 or a route distinguisher (RD)-specific address:
  - If you do not configure the **mpls export vpnv4 prefixes** command, VPN prefixes are not tracked in the MPLS PAL table. These prefixes are displayed by the **show mpls flow mappings** command as 0.0.0.0.
  - If you configure the **mpls export vpnv4 prefixes** command, VPN prefixes are tracked and RD-specific addresses are displayed by the **show mpls flow mappings** command.

# Information About NetFlow MPLS Label Export

The following sections contain useful information for understanding how to configure and use the NetFlow MPLS Label Export feature:

- [MPLS Label Information Gathering and Exporting, page 3](#)
- [Labels Allocated by VPNs, BGP IPv4, or BGP VPNv4 in the MPLS PAL Table, page 4](#)
- [MPLS PAL Table Record Export, page 4](#)
- [MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector, page 6](#)
- [MPLS Label Mapping on a Line Card, page 7](#)

## MPLS Label Information Gathering and Exporting

In a Cisco IOS 12.0S, 12.3T, or 12.4T release that supports the MPLS-Aware NetFlow feature, the mapping of the MPLS label to a prefix and an MPLS application is achieved through the use of the Label Forwarding Information Base (LFIB). You can display this information with the **show ip cache verbose flow** command. These releases do not support the NetFlow MPLS Label Export feature.

In a Cisco IOS 12.2(28)SB release or later release that supports the NetFlow MPLS Label Export feature, the mapping of the MPLS label to a destination prefix or Forwarding Equivalence Class (FEC) and to the MPLS application currently using the label is achieved through the use of an MPLS PAL table. Each supported MPLS application on the router where the NetFlow MPLS Label Export feature is configured registers its label values, prefixes, and owning applications as the labels are allocated. This label-tracking functionality operates on the Route Processor (RP) software.

The MPLS label information (label to prefix and application) mapping is exported to a NetFlow collector at the time when the label is allocated. You can configure periodic export of the full MPLS PAL table to a collector for further processing and analysis through the use of the **mpls export interval** command.

An *interval* argument to the **mpls export interval** command controls the time in minutes between full MPLS PAL table exports to the NetFlow collector. You can configure an interval in the range of 0 to 10080 (1 week) minutes:

- If you want to export MPLS PAL table information only when the label is allocated, then configure this command with a 0 time interval with the **mpls export interval 0** command.
- If you want to trigger an immediate export of the full MPLS PAL table, reconfigure the command with an *interval* argument that is different from the interval that is configured. For example, if you have configured the **mpls export interval 1440** command, reconfigure the command with any nonzero number except 1440.
- If you have a complex network that generates a large amount of traffic, configure a large interval between MPLS PAL table exports. You might want to configure an interval from 6 to 12 hours (360 and 720 minutes).

The *interval* argument that you specify is the least amount of time that passes before another export of the MPLS PAL table occurs. The system could delay the MPLS PAL table export for 10 minutes if the PAL export queue already contains a large number of entries. This could happen if the export occurred at a time when thousands of routes just came up, or if NetFlow did not have the time to clear the export queue from either a previous export of the full table or a previous time when thousands of routes came up in a brief period of time.

After you have entered the **mpls export interval** command, you can use the **show mpls flow mappings** command to display MPLS PAL table entries. To display information about the number of MPLS PAL records exported to the collector, use the **show ip flow export verbose** command.

## Labels Allocated by VPNs, BGP IPv4, or BGP VPNv4 in the MPLS PAL Table

If you want to see VPN prefix information, that is, labels allocated by VPN, BGP IPv4, or BGP VPNv4, you need to configure the **mpls export vpnv4 prefixes** command. If you do not configure the **mpls export vpnv4 prefixes** command, MPLS PAL stores labels allocated by these application as prefix 0.0.0.0.

After you configure the **mpls export vpnv4 prefixes** command, the VPN prefix and the associated RD are stored in the MPLS PAL table. VPN addresses are made unique by adding an RD to the front of the address. The RD removes any ambiguity when the same VPN prefix is used for more than one VRF.



### Note

To export VPN prefixes and associated RDs from the MPLS PAL table, the first time you configure the **mpls export vpnv4 prefixes** command you need to save the configuration and reboot the router or clear all routes from the table.

To display the VPN prefix entries in the MPLS PAL table, use the **show mpls flow mappings** command.

With the **mpls export vpnv4 prefixes** command configured, a line of the output might look like this:

```
Router# show mpls flow mappings
```

Label	Owner	Route-Distinguisher	Prefix	Allocated
.				
.				
27	BGP	100:1	10.34.0.0	00:57:48

The format of the Route-Distinguisher field in the output depends on how the RD was configured. The RD can be configured in the as-number:network number (ASN:nn) format, as shown in the example, or it can be configured in the IP address:network number format (IP-address:nn).

If you did not configure the **mpls export vpnv4 prefixes** command, a line of the output looks like this:

```
Router# show mpls flow mappings
```

.				
.				
.				
Label	Owner	Route-Distinguisher	Prefix	Allocated
21	BGP		0.0.0.0	00:52:18

The Route-Distinguisher field is not populated and the Prefix is displayed as 0.0.0.0.

If the MPLS PAL table tracks a per-VRF aggregate label and you configured the **mpls export vpnv4 prefixes** command, the **show mpls flow mappings** command displays the RD associated with the per-VRF aggregate label, but the prefix for the per-VRF aggregate label is reported as 0.0.0.0. If the **mpls export vpnv4 prefixes** command is not configured, the per-VRF aggregate label is reported with no RD and prefix 0.0.0.0, and you cannot distinguish the per-VRF aggregate label from a normal BGP label.

## MPLS PAL Table Record Export

In Cisco IOS Release 12.0S and later releases, the export of MPLS-Aware NetFlow cache records makes use of the NetFlow Version 9 export format data and template. The export of MPLS PAL table entries also uses the NetFlow Version 9 export format. MPLS PAL packets are exported as NetFlow options packets rather than NetFlow data packets. NetFlow options packets are defined in *Cisco Systems NetFlow Services Export Version 9*, Request for Comments (RFC) 3954.

The RP on the PE router learns and queues the MPLS PAL table records for export. The RP can combine large numbers of PAL table entries in a single Version 9 record and send the record to the NetFlow collector. The information exported by the RP contains instances of the following for each tracked label:

Label, allocating-application (Owner), Route-Distinguisher, Prefix, time stamp (Allocated)

Because the mapping may change as labels expire and are reused, each PAL record contains a time stamp indicating the system uptime at which the label was allocated.

#### **NetFlow Export Template Format Used for MPLS PAL Entries**

This is the NetFlow Version 9 export template format used for MPLS PAL entries:

MPLS label: 3 bytes

MPLS label application type: 1 byte

MPLS label IP prefix: 4 bytes

MPLS VPN prefix RD: 8 bytes

MPLS label allocation time: 4 bytes

#### **MPLS Application Types Exported**

The following MPLS application types are exported in the MPLS label application type field:

TE = 1

ATOM = 2

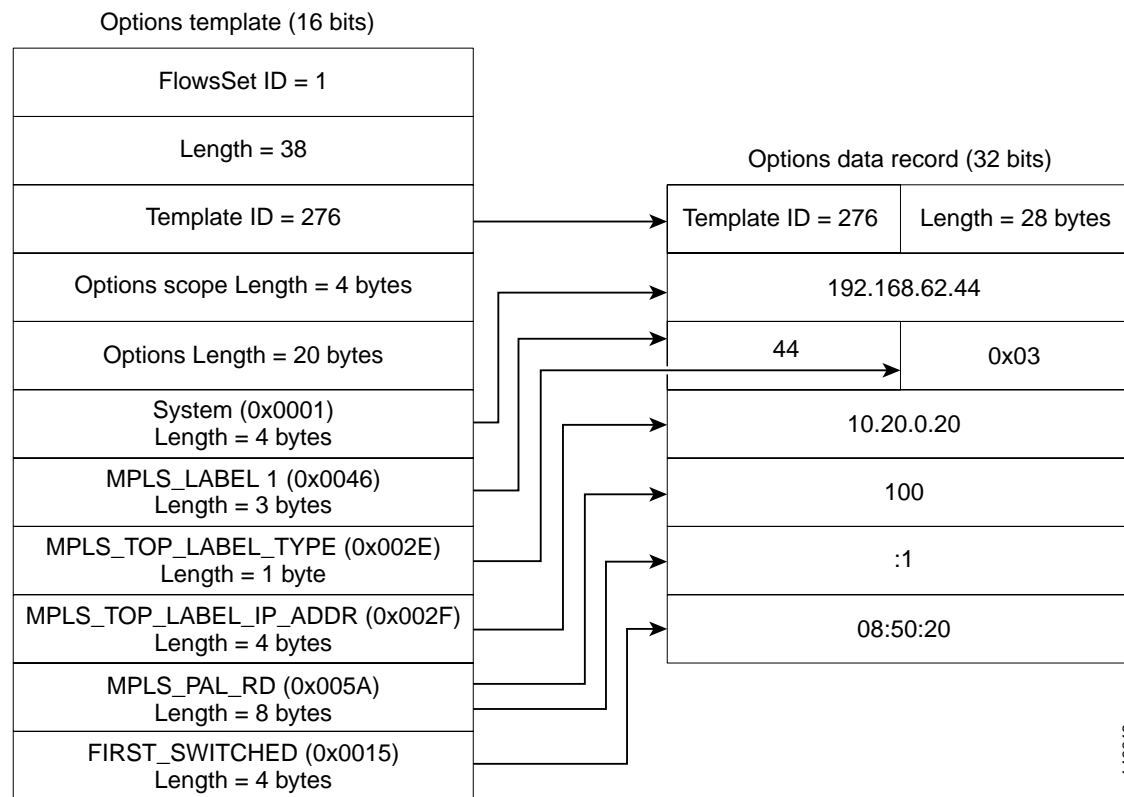
VPN = 3

BGP = 4

LDP = 5

#### **Options Template and Options Data Record for MPLS PAL Record Export**

[Figure 1](#) shows an example of the options template and options data record for MPLS PAL record export. This example shows that MPLS label 44 was allocated by a VPN 0x03 at 08:50:20 and is associated with the IP address 10.20.0.20 and with RD 100:1.

**Figure 1**      **MPLS PAL Export Format Record**

## MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector

A NetFlow collector can gather the PAL NetFlow packets from a PE router and correlate the label mappings with the recent NetFlow records from adjacent provider core (P) routers.

For example, the MPLS PAL export packet contains MPLS label mappings over a period of time, as each label is allocated and reallocated on the PE router. The packet might contain the following information:

```
label 5, prefix 10.0.0.0, type LDP, 12:00:00
label 4, prefix 10.10.0.0, type LDP, 13:00:00
label 5, prefix 10.9.0.0, type VPN, 14:00:00
```

The NetFlow collector then receives a NetFlow packet from the adjacent P router indicating the following:

```
label 5, 123 packets, 9876 bytes, time 12:22:15.
```

The collector would match the time range known from the PAL packets with the line card (LC) packet time stamp. This would result in the correct mapping for label 5 at time 12:22:15, as follows:

```
label 5, application LDP, prefix 10.0.0.0.
```

The NetFlow collector needs to be able to handle relative differences in the time stamps caused by different reboot times of the P and PE routers.



To implement the offline label mapping checks in the NetFlow collector, the collector needs to maintain a history of label mappings obtained from the MPLS PAL NetFlow packets sent by the RP. If a label is deallocated and reallocated, the collector should track both the old and the new MPLS PAL information for the label.

**Note**

On a rare occasion, the collector might not be able to accurately track how many packets flowed for a label that has been deallocated by one application and soon reallocated by another application.

## MPLS Label Mapping on a Line Card

Label to prefix and application mapping is registered and exported from the router RP. This functionality does not occur on the line card. If you want to see the mapping for a particular label on a line card and the label of interest is tracked by the MPLS PAL table, then you can do the following:

- Enter the **show mpls forwarding** command on the line card.
- Enter the **show mpls flow mappings** on the RP.
- Compare the output of the two commands.

You might find the **| include** keyword to the commands useful in this case. For example, You could enter the **show mpls flow mappings | include 777** command to see the information for any label with substring 777.

## How to Configure NetFlow MPLS Label Export

Perform the following tasks to configure the NetFlow MPLS Label Export feature on an LSR. This feature provides the label, prefix, and application mapping through the MPLS PAL table that collects and exports the data to a NetFlow collector.

- [Configuring NetFlow MPLS Label Export and MPLS PAL Table Export, page 7](#) (required)
- [Displaying Information About the MPLS PAL Table, page 9](#) (optional)
- [Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector, page 10](#) (optional)

## Configuring NetFlow MPLS Label Export and MPLS PAL Table Export

Perform this task to configure the NetFlow MPLS Label Export feature and MPLS PAL table export to a NetFlow collector. You can use the information generated for network traffic planning and billing.

The following task must be completed before MPLS labels are allocated by the router for the MPLS PAL table to be exported to a NetFlow collector.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls export interval *interval***
4. **end**

5. `copy running-config startup-config`
6. `exit`
7. Reboot the router.

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>mpls export interval interval</code>  <b>Example:</b> <code>Router(config)# mpls export interval 360</code>	Configures a periodic time interval for the export of the entire MPLS PAL table to a NetFlow collector. <ul style="list-style-type: none"> <li>The <i>interval</i> argument specifies the time in minutes between full PAL table exports. The range of valid time intervals is 0 to 10,080 minutes.</li> <li>We recommend that you select a time interval from 360 minutes (6 hours) to 1440 minutes (24 hours) depending on the size of your network and how often the NetFlow collector might be restarted.</li> <li>If you enter an interval of 0, full PAL table exports are disabled. PAL information is exported only as labels are allocated.</li> <li>If you need to restart your NetFlow collector and want to learn PAL information immediately, you can change the <i>interval</i> argument. When you change the time interval, the application exports the full PAL table.</li> </ul> <b>Note</b> Allocated labels are tracked only after you enter the <b>mpls export interval</b> command. Any labels allocated before you enter this command are not tracked.
Step 4	<code>end</code>  <b>Example:</b> <code>Router(config)# end</code>	Exits to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>  <b>Example:</b> <code>Router# copy running-config startup-config</code>	Copies the modified configuration into router NVRAM, permanently saving the settings.  The next time the router is reloaded or rebooted the NetFlow MPLS Label Export feature is already part of the configuration.

	Command or Action	Purpose
Step 6	<code>exit</code>  <b>Example:</b> <code>Router# exit</code>	Exits to user EXEC mode.
Step 7	Reboot the router.	(Optional) Saves the configuration and reboots the router to ensure that the information collected by this feature is complete.

## Displaying Information About the MPLS PAL Table

Perform this task to display information about the MPLS PAL table. The information displayed includes the label, the application that allocated the label, an RD and destination prefix associated with the label, and the time the label was allocated by the application.

### SUMMARY STEPS

1. `enable`
2. `show mpls flow mappings`
3. `show ip flow export verbose | include PAL`
4. `exit`

### DETAILED STEPS

#### Step 1 `enable`

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

#### Step 2 `show mpls flow mappings`

Use this command to display entries in the MPLS PAL table. For example:

```
Router# show mpls flow mappings
```

Label	Owner	Route-Distinguisher	Prefix	Allocated
18	LDP		10.0.0.5	00:52:10
21	BGP		0.0.0.0	00:52:18
22	BGP		0.0.0.0	00:52:18
25	BGP		0.0.0.0	00:51:44
26	LDP		10.32.0.0	00:52:10
27	TE-MIDPT		10.30.0.2	00:52:06
28	LDP		10.33.0.0	00:52:10
29	LDP		10.0.0.1	00:52:10
30	LDP		10.0.0.3	00:52:10

In this example, the `mpls export vpnv4 prefixes` command was not configured. Therefore, the MPLS PAL functionality did not export an RD for the BGP application, and the associated prefix is exported as 0.0.0.0.

The following shows sample output from the `show mpls flow mappings` command if you previously entered the `mpls export vpnv4 prefixes` command:

```
Router# show mpls flow mappings
```

Label	Owner	Route-Distinguisher	Prefix	Allocated
16	LDP		10.0.0.3	00:58:03
17	LDP		10.33.0.0	00:58:03
19	TE-MIDPT		10.30.0.2	00:58:06
20	LDP		10.0.0.5	00:58:03
23	LDP		10.0.0.1	00:58:03
24	LDP		10.32.0.0	00:58:03
27	BGP	100:1	10.34.0.0	00:57:48
31	BGP	100:1	10.0.0.9	00:58:21
32	BGP	100:1	10.3.3.0	00:58:21

### Step 3 show ip flow export verbose | include PAL

Use this command to display the number of MPLS PAL records that were exported to the NetFlow collector. For example:

```
Router# show ip flow verbose | include PAL
```

```
6 MPLS PAL records exported
```

When you specify the **verbose** keyword and MPLS PAL records have been exported using NetFlow Version 9 data format, the command output contains an additional line that precedes the “x records exported in y UDP datagrams” line.

### Step 4 exit

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector

Perform the following task to configure the export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.

This allows you to track VPN prefix information for MPLS labels allocated by VPNs, BGP IPv4, and BGP VPNv4. You can use the data analyzed by the collector to assist in network traffic planning and billing.

### Prerequisites

A VRF must be configured on the router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls export interval *interval***
4. **mpls export vpnv4 prefixes**

5. **end**
6. **copy running-config startup-config**
7. **exit**
8. Reboot the router.
9. **enable**
10. **show mpls flow mappings**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls export interval interval</b>  <b>Example:</b> Router(config)# mpls export interval 1440	Configures the collection and export of MPLS PAL information to a NetFlow collector. <ul style="list-style-type: none"> <li>The <i>interval</i> argument specifies the time in minutes between full PAL table exports. The range of valid time intervals is 0 to 10,080 minutes.</li> <li>We recommend that you select a time interval of 6 hours (360 minutes) to 24 hours (1440 minutes) depending on the size of your network.</li> <li>If you enter an interval of 0, full PAL table exports are disabled. PAL information is exported only as labels are allocated.</li> <li>If you need to restart your NetFlow collector and want to learn PAL information immediately, you can change the <i>interval</i> argument. When you change the time interval, the application exports the full PAL table.</li> </ul>
Step 4	<b>mpls export vpnv4 prefixes</b>  <b>Example:</b> Router(config)# mpls export vpnv4 prefixes	Configures the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector.
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

	Command or Action	Purpose
<b>Step 6</b>	<code>copy running-config startup-config</code>  <b>Example:</b> Router# <code>copy running-config startup-config</code>	Copies the modified configuration into router NVRAM, permanently saving the settings.  The next time the router is rebooted the tracking and export of VPNv4 label information from the MPLS PAL table to a NetFlow collector is already part of the configuration.
<b>Step 7</b>	<code>exit</code>  <b>Example:</b> Router# <code>exit</code>	Exits to user EXEC mode.
<b>Step 8</b>	Reboot the router.	(Optional) Saves the configuration and reboots the router to ensure that the information collected by this feature is complete.
<b>Step 9</b>	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 10</b>	<code>show mpls flow mappings</code>  <b>Example:</b> Router# <code>show mpls flow mappings</code>	Displays MPLS PAL table entries that include VPNv4 prefixes and VPN RDs.

## Configuration Examples for NetFlow MPLS Label Export

This section contains the following configuration examples for the NetFlow MPLS Label Export feature:

- [Configuring NetFlow MPLS Prefix/Application/Label Table Export: Examples, page 12](#)
- [Configuring the Export of MPLS VPNv4 Label Information from the MPLS PAL Table: Example, page 13](#)

### Configuring NetFlow MPLS Prefix/Application/Label Table Export: Examples

The following examples show how to configure NetFlow MPLS PAL table export on a PE router.

This example shows how to configure the export of the full MPLS PAL table every 480 minutes (8 hours):

```
configure terminal
!
mpls export interval 480
end
copy running-config startup-config
exit
```

This example shows how to configure MPLS PAL information export only as the labels are allocated:

```
configure terminal
!
mpls export interval 0
end
```

```
copy running-config startup-config
exit
```

In this example, the full MPLS PAL table is not exported repeatedly.

## Configuring the Export of MPLS VPNv4 Label Information from the MPLS PAL Table: Example

The following example shows how to configure the export of MPLS VPNv4 label information from the MPLS PAL table:

```
configure terminal
!
mpls export interval 720
mpls export vpnv4 prefixes
end
copy running-config startup-config
exit
```

The full MPLS PAL table with MPLS VPNv4 label information is configured to export to the NetFlow collector every 720 minutes (12 hours).

## Additional References

The following sections provide references related to the NetFlow MPLS Label Export feature.

### Related Documents

Related Topic	Document Title
Tasks for configuring MPLS-aware NetFlow	<a href="#">Configuring MPLS-aware NetFlow</a>
Overview of the NetFlow application and advanced NetFlow features and services	<a href="#">Cisco IOS NetFlow Overview</a>
Tasks for configuring NetFlow to capture and export network traffic data	<a href="#">Configuring NetFlow and NetFlow Data Export</a>
Tasks for configuring MPLS egress NetFlow accounting	<a href="#">Configuring MPLS Egress NetFlow Accounting</a>
Detailed information about the fields available in Version 9 export format and about export format architecture	<a href="#">Cisco IOS NetFlow Version 9 Flow-Record Format</a>

### Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3954	<i>Cisco Systems NetFlow Services Export Version 9</i>
RFC 2547	<i>BGP/MPLS VPNs</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>



# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **mpls export interval**
- **mpls export vpnv4 prefixes**
- **show ip flow export**
- **show mpls flow mappings**

# Feature Information for NetFlow MPLS Label Export

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

**Table 1** Feature Information for NetFlow MPLS Label Export

Feature Name	Releases	Feature Information
NetFlow MPLS Label Export	12.2(28)SB 12.2(33)SRA	<p>The NetFlow MPLS Label Export feature provides the label switch router (LSR) with the capability of collecting and exporting the top label in the MPLS label stack along with its prefix or Forwarding Equivalence Class (FEC) and the application allocating the label to a NetFlow collector for supported MPLS applications.</p> <p>In 12.2(28)SB, this feature was introduced.</p> <p>In 12.2(33)SRA, this feature was integrated into a 12.2SRA release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS Label Information Gathering and Exporting, page 3</a></li> <li>• <a href="#">Labels Allocated by VPNs, BGP IPv4, or BGP VPNv4 in the MPLS PAL Table, page 4</a></li> <li>• <a href="#">MPLS PAL Table Record Export, page 4</a></li> <li>• <a href="#">MPLS PAL and NetFlow Statistics Correlation on a NetFlow Collector, page 6</a></li> <li>• <a href="#">MPLS Label Mapping on a Line Card, page 7</a></li> <li>• <a href="#">Configuring NetFlow MPLS Label Export and MPLS PAL Table Export, page 7</a></li> <li>• <a href="#">Displaying Information About the MPLS PAL Table, page 9</a></li> <li>• <a href="#">Configuring the Export of MPLS VPN Version 4 Label Information from the MPLS PAL Table to a NetFlow Collector, page 10</a></li> </ul>

# Glossary

**BGP**—Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. It is defined by RFC 1163.

**export packet**—A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

**FEC**—Forward Equivalency Class. A set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC. A flow is another example.

**flow**—A unidirectional stream of packets between a given source and destination—each of which is defined by a network-layer IP address and transport-layer source and destination port numbers. A unique flow is defined as the combination of the following key fields: source IP address, destination IP address, source port number, destination port number, Layer 3 protocol type, type of service (ToS), and input logical interface.

**flowset**—A collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

**IPv6**—IP Version 6. Replacement for IP Version 4 (IPv4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

**label**—A short, fixed-length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

**LDP**—Label Distribution Protocol. A standard protocol that operates between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LFIB**—Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSR**—label switch router. A router that forwards packets in a Multiprotocol Label Switching (MPLS) network by looking only at the fixed-length label.

**MPLS**—Multiprotocol Label Switching. A switching method in which IP traffic is forwarded through use of a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

**NetFlow**—A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

**NetFlow Collection Engine** (formerly NetFlow FlowCollector)—A Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

**NetFlow v9**—NetFlow export format Version 9. A flexible and extensible means of carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

**network byte order**—Internet-standard ordering of the bytes corresponding to numeric values.

**options data record**—Special type of data record that is used in the NetFlow process. It is based on an options template and has a reserved template ID that provides information about the NetFlow process itself.

**options template**—A type of template record that the router uses to communicate the format of NetFlow-related data to the NetFlow collector.

**P router**—provider core or backbone router. A router that is part of a service provider's core or backbone network and is connected to the provider edge (PE) routers.

**packet header**—First part of an export packet. It provides basic information about the packet (such as the NetFlow version, number of records contained in the packet, and sequence numbering) so that lost packets can be detected.

**PAL table**—Prefix/Application/Label table. A data structure that collects and exports the prefix, application, and time stamp for a specific label.

**PE router**—provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Virtual Private Network (VPN) processing occurs in the PE router.

**RD**—route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.

There are two formats for configuring the route distinguisher argument. It can be configured in the as-number:network number (ASN:nn) format or it can be configured in the IP address:network number format (IP-address:nn).

**RP**—Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a Supervisory Processor.

**TE**—traffic engineering. Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**TE tunnel**—traffic engineering tunnel. A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path.

**template flowset**—A collection of template records that are grouped in an export packet.

**template ID**—A unique number that distinguishes a template record produced by an export device from other template records produced by the same export device. A NetFlow Collection Engine application can receive export packets from several devices. You should be aware that uniqueness is not guaranteed across export devices. Thus, you should configure the NetFlow Collection Engine to cache the address of the export device that produced the template ID in order to enforce uniqueness.

**VPN**—Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

**VPNv4 prefix**—IPv4 prefix preceded by an 8-byte route distinguisher. The VPN addresses are made unique by adding a route distinguisher to the front of the address.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.





# ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

---

**First Published:** January 01, 2006  
**Last Updated:** October 02, 2009

This feature allows you to configure multiple VCs that have different quality of service (QoS) characteristics between any pair of ATM-connected routers that support this feature. VC bundle management allows multiple VCs with various QoS settings to be directed to the same destination and to map traffic to the VCs based on protocol criteria associated with the traffic. Three experimental (EXP) bits in the Multiprotocol Label Switching (MPLS) packets determine which VC in the bundle to use to forward the packets.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection”](#) section on page 27.

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

## Contents

- [Prerequisites for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection](#), page 2
- [Restrictions for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection](#), page 2
- [Information About ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection](#), page 2
- [How to Configure ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection](#), page 6



---

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

- [Configuration Examples for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection, page 22](#)
- [Additional References, page 25](#)
- [Feature Information for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection, page 27](#)

## Prerequisites for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

This feature requires ATM VC management, Cisco Express Forwarding, and Forwarding Information Base (FIB) and Label Forwarding Information Base (LFIB) switching functionality.

## Restrictions for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

- The router at the remote end must be running a version of Cisco IOS software that supports MPLS and ATM VC management.
- This feature is not supported on either the ATM interface processor (AIP) or the ATM Lite port adapter (PA-A1).

## Information About ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

You need to understand the concepts in the following sections to configure the MPLS EXP Bits Based ATM PVC Bundles VC Selection feature:

- [ATM VC Bundle Management, page 2](#)
- [ATM VC Bundle Configuration, page 3](#)
- [Benefits of ATM VC Bundle Management, page 4](#)
- [VC Bundle Management Supported Features, page 5](#)

## ATM VC Bundle Management

The MPLS EXP Bits Based ATM PVC Bundles VC Selection feature is an extension to the IP to ATM Class of Service feature suite. The IP to ATM Class of Service feature suite, using VC support and bundle management, maps QoS characteristics between IP and ATM. It provides customers that have multiple VCs (with varying qualities of service to the same destination) the ability to build a QoS differentiated network.

The IP to ATM Class of Service feature suite allows customers to use IP precedence level as the selection criterion for packet forwarding. This feature provides customers with the option of using the MPLS experimental level as an additional selection criterion for packet forwarding.



**Note**

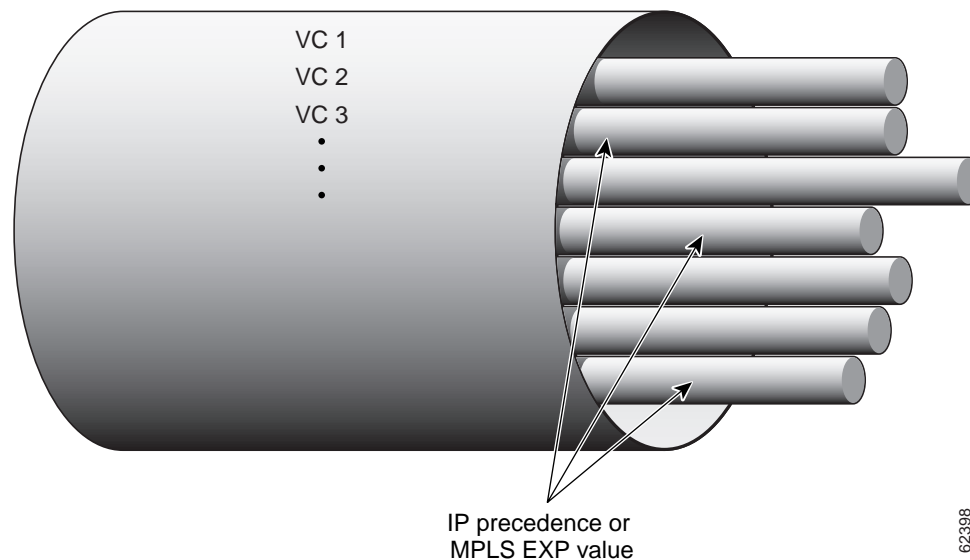
If a selection criterion for packet forwarding is not selected (that is, if the packet is unlabeled), this feature uses the IP precedence level as the default selection criterion.

For more information about the IP to ATM Class of Service feature suite, see the [“Related Documents” section on page 25](#).

## ATM VC Bundle Configuration

ATM VC bundle management allows you to configure multiple VCs that have different QoS characteristics between any pair of ATM-connected routers. As shown in [Figure 1](#), these VCs are grouped in a bundle and are referred to as bundle members.

**Figure 1**      **ATM VC Bundle**



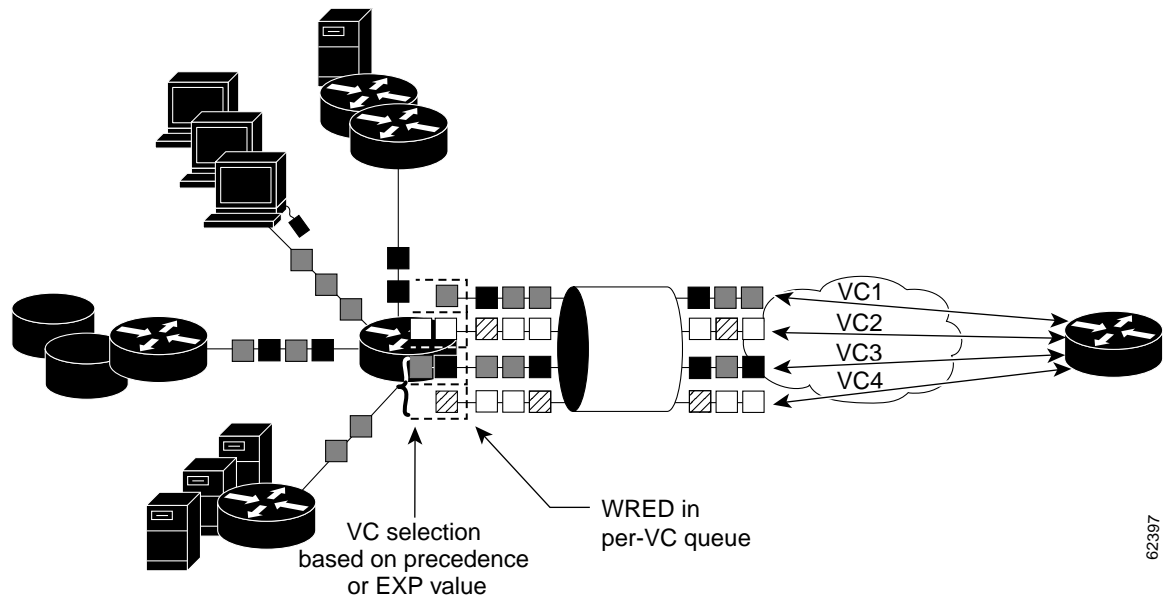
ATM VC bundle management allows you to define an ATM VC bundle and add VCs to it. Each VC of a bundle has its own ATM traffic class and ATM traffic parameters. You can apply attributes and characteristics to discrete VC bundle members, or you can apply them collectively at the bundle level.

Using VC bundles, you can create differentiated service by flexibly distributing MPLS EXP levels over the different VC bundle members. You can map a single MPLS EXP level, or a range of these levels, to each discrete VC in the bundle, thereby enabling individual VCs in the bundle to carry packets marked with different MPLS EXP levels. You can use Weighted Random Early Detection (WRED) or distributed WRED (dWRED) to further differentiate service across traffic that has different MPLS EXP levels.

To determine which VC in the bundle to use to forward a packet to its destination, the ATM VC bundle management software matches MPLS EXP levels between packets and VCs (see [Figure 2](#)). IP traffic is sent to the next hop address for the bundle because all VCs in a bundle share the same destination, but the VC used to carry a packet depends on the value set for that packet in the MPLS EXP level of the type of service (ToS) byte of its header. The ATM VC bundle management software matches the MPLS EXP level of the packet to the MPLS EXP levels assigned to a VC, sending the packet out on the appropriate VC.

Moreover, the ATM VC bundle management software allows you to configure how traffic will be redirected when the VC to which the packet was initially directed goes down. [Figure 2](#) illustrates how the ATM VC bundle management software determines which permanent virtual circuit (PVC) bundle member to use to carry a packet and how WRED (or dWRED) is used to differentiate traffic on the same VC.

**Figure 2** *ATM VC Bundle PVC Selection for Packet Transfer*



The support of multiple parallel ATM VCs allows you to create stronger service differentiation at the IP layer. For example, you might want to configure the network to provide IP traffic belonging to real-time class of service (CoS) such as Voice over IP traffic on an ATM VC with strict constraints on constant bit rate (CBR) or variable bit rate real-time (VBR-rt), while also allowing the network to transport nonreal-time traffic over a more elastic ATM unspecified bit rate (UBR) PVC. UBR is effectively the ATM version of best-effort service. Using a multiple parallel ATM VC configuration allows you to make full use of your network capacity.

## Benefits of ATM VC Bundle Management

ATM VC bundle management was designed to provide a true working solution to class-based services, without the investment of new ATM network infrastructures. It allows networks to offer different service classes (sometimes termed differential service classes) across the entire WAN, not just the routed portion. Mission-critical applications can be given exceptional service during periods of high network usage and congestion. In addition, noncritical traffic can be restricted in its network usage, ensuring greater QoS for more important traffic and user types.

ATM VC bundle management gives customers the option of using the MPLS EXP level, in addition to IP precedence, as a selection criterion for packet forwarding.

## VC Bundle Management Supported Features

The following features are supported on an MPLS over VC bundle:

- PVC support only (no switched virtual circuits or SVCs):
  - Support for multipoint and point-to-point subinterfaces.
  - Support for AAL5SNAP (RFC1483 bridging) and multiplex (MUX) type VCs encapsulation.
  - Use of static mapping and Inverse Address Resolution Protocol (Inverse ARP) for the next hop protocol address (supported on multipoint subinterfaces only).
  - PVCs associated with VC bundles through explicit configuration.
  - Use of Interim Local Management Interface (ILMI) and Operation, Administration, and Maintenance (OAM) functionality in the PVC management feature for PVC failure detection.
- VC selection within the bundle:
  - Uses three EXP bits in the MPLS header to define the precedence levels, with level 7 being the highest for MPLS traffic.
  - No automapping of VCs to precedence levels can be done. The user must use the **mpls experimental** command under each member VC to explicitly specify the mapping.
  - Multiple precedence levels can be mapped to one VC.
  - Packets with the PAK\_PRIORITY\_CRUCIAL flag set go on a high precedence (level 6) VC. These packets include IP routing packets such as Intermediate System-Intermediate System (IS-IS) packets for integrated IP routing. Label Distribution Protocol (LDP) and Tag Distribution Protocol (TDP) messages, and Inverse ARP packets also use a precedence level 6 VC. However, OAM cells still flow in the individual VC to detect PVC failures, although the PAK\_PRIORITY\_CRUCIAL flag is set for them.
  - Regular **ping** commands use the lowest precedence (level 0) VC. If other protocols such as Internetwork Packet Exchange (IPX) are configured in the bundle, they will also use the lowest precedence level VC for their traffic.
- ATM Inverse ARP:
  - Inverse ARP is viewed as a parameter at the bundle level and can be enabled or disabled only for the bundle, not for individual VCs in the bundle.
  - The PAK\_PRIORITY\_CRUCIAL flag is set in each ATM Inverse ARP packet and the packets use the precedence level 6 VC.
  - Inverse ARP for other protocols such as IPX is off by default unless it is configured in the bundle.
- Broadcast and multicast:
  - Broadcasting can be turned on or off at the bundle level, not at the individual VC level in the bundle.
  - Pseudobroadcasting is used for forwarding the broadcast traffic.
  - VC selection for the broadcast traffic is based on the precedence levels of the broadcast packets.
- Bundle management:
  - According to the protected group rule, when all members in the protected group fail, the bundle is declared down.
  - According to the protected VC rule, when a protected VC goes down, the bundle goes down.
  - A VC can be a standalone VC or belong to only one bundle.

- When a bundle goes down, no traffic should be forwarded out the bundle, even if some of the VCs in the bundle are still up.
- In VC bumping, each bundle member can specify if bumping is allowed. If bumping is allowed, the next lower precedence level VC is selected when a VC goes down. This is the implicit bumping rule. Traffic is restored to the original VC when it comes back.
- In explicit VC bumping, a VC can specify to which precedence level it wants to bump its traffic when it goes down. Only one precedence level can be specified for bumping. If the VC that carries the bumped traffic also fails, the traffic will follow the bumping rules specified for that VC.
- In reject bumping, a VC may also be configured not to accept the bumped traffic.
- When no alternate VC can be found for some bumped traffic, the bundle has to be declared down.
- To avoid bringing down a bundle because of a failure of the lowest precedence VC, configure explicit bumping on the lowest precedence VC.
- Bundle status attributes and their current status for each VC in the bundle can be displayed in a tabular form using EXEC commands.
- Bundle statistics are the same statistics provided for VC that have been aggregated for a VC bundle.
- Bundle debugging commands, when enabled, print bundle events and bundle errors.
- Packet forwarding:
  - There are four possible paths for MPLS packet forwarding over the VC bundle: IP to MPLS, MPLS to MPLS, MPLS to IP, and locally generated packets.
  - Process switching is used for locally generated packets.
  - Cisco Express Forwarding FIB switching is used for the IP to MPLS path.
  - Cisco Express Forwarding LFIB switching is used for the MPLS to MPLS and MPLS to IP paths.
  - No fast switching is supported for transit IP packets. The fast switching path does not classify IP packets based on their precedence levels.
  - VC bundle configuration is already added to handle the IP VC bundle feature and may be used without any modification.

## How to Configure ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

This section contains the following procedures:

- [Configuring MPLS and Creating a VC Bundle, page 7](#) (required)
- [Configuring the Bundle-Level Protocol, page 9](#) (required)
- [Configuring Parameters on a VC Bundle Member Directly, page 9](#) (optional)
- [Configuring a VC Class and Applying Parameters to a Bundle, page 11](#) (optional)
- [Attaching a Class to a Bundle, page 14](#) (optional)
- [Configuring a VC Bundle at the Subinterface Level, page 15](#) (optional)

- [Assigning VC and Bundle Attributes, page 18](#) (optional)
- [Verifying ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection Configuration, page 21](#) (optional)

## Configuring MPLS and Creating a VC Bundle

Perform this task to enable MPLS and create a VC bundle. When you create a VC bundle, you enter bundle configuration mode, in which you can assign attributes and parameters to the bundle and to all of its member VCs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp advertise-labels**
5. **interface atm** *interface-number* [*subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
6. **ip address** *ip-address mask*
7. **mpls ip**
8. **bundle** *bundle-name*

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef	Enables Cisco Express Forwarding, which is needed for MPLS.  <b>Note</b> This command without the optional keyword enables Cisco Express Forwarding on the Route Processor (RP) card. The optional <b>distributed</b> keyword is used to enable distributed Cisco Express Forwarding for the Versatile Interface Processor (VIP)-based platforms.
Step 4	<b>mpls ldp advertise-labels</b>  <b>Example:</b> Router(config)# mpls ldp advertise-labels	Controls the distribution of locally assigned, incoming labels by means of the LDP, and allows TDP neighbors to exchange messages between them.

	Command or Action	Purpose
<b>Step 5</b>	<pre>interface atm interface-number[.subinterface-number {mpls   multipoint   point-to-point}]</pre> <p><b>Example:</b> Router(config)# interface atm 0/0/3</p>	Configures an ATM interface and enters interface configuration mode.
<b>Step 6</b>	<pre>ip address ip-address mask</pre> <p><b>Example:</b> Router(config-if)# ip address 10.13.11.3 255.255.0.0</p>	Sets the IP address for an interface.
<b>Step 7</b>	<pre>mpls ip</pre> <p><b>Example:</b> Router(config-if)# mpls ip</p>	Enables MPLS forwarding of IP packets along normally routed paths for the platform.
<b>Step 8</b>	<pre>bundle bundle-name</pre> <p><b>Example:</b> Router(config-if)# bundle new-york</p>	Creates or modifies a bundle and enters bundle configuration mode. The prompt changes to the following:  Router(config-if-atm-bundle)#

## What to Do Next

Decide whether you want to configure the VC bundle member directly or use a VC class attached to a bundle.

You can apply parameters (or attributes) to bundles either by applying the parameters directly to the bundle or by applying the parameters to a VC class assigned to the bundle.

Applying parameters by using VC classes assigned to the bundle allows you to apply multiple parameters at once because you apply the VC class to the bundle and to all of its VC members. This method allows you to apply a parameter across all VCs for the bundle, after which (for some parameters) you can later modify that parameter for individual VCs. After configuring the parameters for the VC class, you need to attach the VC class to the bundle.

To configure the VC bundle member directly, complete the procedure in the [“Configuring Parameters on a VC Bundle Member Directly”](#) section on page 9. To use a VC class attached to a bundle, instead complete the procedures in both the [“Configuring a VC Class and Applying Parameters to a Bundle”](#) section and the [“Attaching a Class to a Bundle”](#) section on page 14.

Parameters applied directly to a bundle take priority over those applied to VC classes assigned to the bundle, and the steps for this task are in the [“Configuring the Bundle-Level Protocol”](#) section on page 9. Parameters applied to VC classes assigned to the bundle take priority over those applied to individual VCs.



### Note

Some parameters applied through a VC class or directly to the bundle can be superseded by commands that you apply directly to individual VCs in bundle-VC configuration mode.

## Configuring the Bundle-Level Protocol

Perform this task to configure a protocol that applies to the bundle and to all of its members. The commands in these steps are entered in bundle configuration mode.

### SUMMARY STEPS

1. **protocol** *protocol* [*protocol-address* | **inarp**] [[**no**] **broadcast**]
2. **encapsulation** [**aal5mux** | **aal5snap**]

### DETAILED STEPS

Command or Action	Purpose
<b>Step 1</b> <b>protocol</b> <i>protocol</i> [ <i>protocol-address</i>   <b>inarp</b> ] [[ <b>no</b> ] <b>broadcast</b> ]  <b>Example:</b> Router(config-if-atm-bundle)# <b>protocol</b> <i>clns</i> 10.0000.0000.0000.3333.00 <b>broadcast</b>	Configures a static map (the map statement for the bundle) for an ATM PVC, SVC, or VC class. <ul style="list-style-type: none"> <li>• <i>protocol</i>—Networking protocol.</li> <li>• <i>protocol-address</i>—Destination address that is being mapped to a PVC.</li> <li>• <b>inarp</b>—(Valid only for IP and IPX protocols on PVCs) Enables Inverse ARP on an ATM PVC. If you specify a protocol address instead of the <b>inarp</b> keyword, Inverse ARP is automatically disabled for that protocol.</li> <li>• [[<b>no</b>] <b>broadcast</b>—Indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface.</li> </ul> <b>Note</b> Pseudobroadcasting is supported. The <b>broadcast</b> keyword of the <b>protocol</b> command takes precedence if you previously configured the <b>broadcast</b> command on the ATM PVC or SVC.
<b>Step 2</b> <b>encapsulation</b> [ <b>aal5mux</b>   <b>aal5snap</b> ]  <b>Example:</b> Router(config-if-atm-bundle)# <b>encapsulation</b> <b>aal5snap</b>	Configures the ATM adaptation layer (AAL) and encapsulation type for every VC in the bundle. <ul style="list-style-type: none"> <li>• <b>aal5mux</b>—AAL and encapsulation type for multiplex (MUX) type VCs. A protocol must be specified when using this encapsulation type.</li> <li>• <b>aal5snap</b>—AAL and encapsulation type that supports Inverse ARP.</li> </ul>

## Configuring Parameters on a VC Bundle Member Directly

Perform this task to configure parameters on an individual VC bundle member directly. The commands in these steps are entered in bundle-VC configuration mode.

### SUMMARY STEPS

1. **pvc-bundle** *pvc-name* [**vpi**]/[**vci**]
2. **ubr** *pcr*

3. **vbr-nrt** *pcr scr [mbs]*
4. **mpls experimental** [*other* | *range*]
5. **bump** {*implicit* | *explicit precedence-level* | **traffic**}
6. **protect** {*group* | **vc**}
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>pvc-bundle</b> <i>pvc-name</i> [<i>vpi</i>/][<i>vci</i>]</p> <p><b>Example:</b>  Router(config-if-atm-bundle)# pvc-bundle  ny-control 207</p>	<p>Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure VC specific parameters.</p> <ul style="list-style-type: none"> <li>The VC is created upon exiting the mode.</li> <li><b>vpi</b>—ATM network virtual path identifier (VPI) for this PVC. The absence of the slash mark (/) and a VPI value defaults the value to 0. The <b>vpi</b> and <b>vci</b> keywords cannot both be set to 0.</li> <li><b>vci</b>—ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the <b>atm vc-per-vp</b> command.</li> </ul> <p><b>Note</b> The <b>pvc-bundle</b> command is used instead of the <b>pvc</b> command to avoid the ambiguity between this command and the interface <b>pvc</b> command.</p>
Step 2	<p><b>ubr</b> <i>pcr</i></p> <p><b>Example:</b>  Router(config-if-atm-member)# ubr 10000</p>	<p>Configures UBR QoS and specifies the output peak cell rate (PCR) for the VC bundle member.</p>
Step 3	<p><b>vbr-nrt</b> <i>pcr scr [mbs]</i></p> <p><b>Example:</b>  Router(config-if-atm-member)# vbr-nrt 20000  10000 32</p>	<p>Configures variable bit rate non-real-time (VBR-nrt) QoS with a PCR, a sustaining cell rate (SCR), and maximum burst size (MBS).</p>
Step 4	<p><b>mpls experimental</b> [<i>other</i>   <i>range</i>]</p> <p><b>Example:</b>  Router(config-if-atm-member)# mpls  experimental 7</p>	<p>Configures MPLS EXP levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle.</p> <ul style="list-style-type: none"> <li>This command is ignored if the class that contains it is not attached to a bundle member.</li> <li><b>other</b>—Any precedence level from 0 to 7 not explicitly configured.</li> <li><b>range</b>—An MPLS EXP level specified as a number or a range of numbers. Ranges can be expressed with a hyphen (2-5, for example), and numbers and ranges can be expressed in groups separated by commas; 1, 3, 5-7, for example.</li> </ul>



	Command or Action	Purpose
Step 5	<b>bump</b> { <b>implicit</b>   <b>explicit</b> <i>precedence-level</i>   <b>traffic</b> }  <b>Example:</b> Router(config-if-atm-member)# bump explicit 7	Configures the bumping rules and applies only to bundle members. <ul style="list-style-type: none"> <li>• <b>implicit</b>—Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC-class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level.</li> <li>• <b>explicit</b> <i>precedence-level</i>—Specifies a precedence level from 0 to 7 for the traffic to be bumped to.</li> <li>• <b>traffic</b>—Specifies that the VC or PVC accepts bumped traffic (the default condition). The <b>no</b> form of this command stipulates that the VC or PVC does not accept any bumped traffic.</li> </ul>
Step 6	<b>protect</b> { <b>group</b>   <b>vc</b> }  <b>Example:</b> Router(config-if-atm-member)# protect vc	Configures a VC class with protected group or protected VC status for application to a VC bundle member. <ul style="list-style-type: none"> <li>• This command makes a bundle member part of the protected group of a bundle or a protected VC in a bundle.</li> <li>• <b>group</b>—Configures the VC or PVC bundle member as part of the protected group of the bundle.</li> <li>• <b>vc</b>—Configures the VC or PVC member as individually protected.</li> </ul>
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if-atm-member)# exit	Exits the current configuration mode. <ul style="list-style-type: none"> <li>• Continue entering <b>exit</b> at the prompt to exit each configuration mode.</li> </ul>

## Configuring a VC Class and Applying Parameters to a Bundle

Perform this task to configure a VC class to contain commands that configure all VC members of a bundle when the class is applied to that bundle. The parameters are applied in VC-class configuration mode. Use the **vc-class atm** command in global configuration mode to enter the VC-class configuration mode.

### Commands Ignored in a VC Class Bundle

When a VC is part of a bundle, some of the VC configuration in the VC class will no longer be applicable to the VC and will be ignored. The inheritance rule for VCs in VC bundles follows this order: VC configuration, bundle configuration, subinterface configuration. In VC mode and bundle mode, the configuration with the individual command takes precedence over the configuration with the **class** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **oam-bundle** [**manage**] [*frequency*]
5. **mpls experimental** [**other** | *range*]
6. **bump** {**implicit** | **explicit** *precedence-level* | **traffic**}
7. **protect** {**group** | **vc**}
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>vc-class atm</b> <i>name</i>  <b>Example:</b> Router(config)# vc-class atm bundle-class	Creates a VC class for an ATM interface and enters VC-class configuration mode.
Step 4	<b>oam-bundle</b> [ <b>manage</b> ] [ <i>frequency</i> ]  <b>Example:</b> Router(config-vc-class)# oam-bundle manage 3	Enables end-to-end F5 OAM loopback cell generation and determines whether the bundle is OAM managed, that is, whether every VC in the bundle is OAM managed. There is no effect if the VC class that contains this command is not attached to a bundle. <ul style="list-style-type: none"> <li><b>manage</b>—Enables OAM management. If this keyword is omitted, loopback cells are sent, but the bundle is not managed.</li> <li><i>frequency</i>—Seconds between transmitted OAM loopback cells. Default is 10 seconds.</li> </ul>

Command or Action	Purpose
<p><b>Step 5</b></p> <pre>mpls experimental [<i>other</i>   <i>range</i>]</pre> <p><b>Example:</b> Router(config-vc-class)# mpls experimental 7</p>	<p>Configures MPLS EXP levels for a VC class that can be assigned to a VC bundle and thus applied to all VC members of that bundle.</p> <ul style="list-style-type: none"> <li>This command is ignored if the class that contains it is not attached to a bundle member.</li> <li><b>other</b>—Any precedence level from 0 to 7 not explicitly configured.</li> <li><b>range</b>—An MPLS EXP level specified as a number or a range of numbers. Ranges can be expressed with a hyphen (2-5, for example), and numbers and ranges can be expressed in groups separated by commas; 1, 3, 5-7, for example.</li> </ul>
<p><b>Step 6</b></p> <pre>bump {implicit   explicit <i>precedence-level</i>   traffic}</pre> <p><b>Example:</b> Router(config-vc-class)# no bump traffic</p>	<p>Configures the bumping rules and applies only to bundle members.</p> <ul style="list-style-type: none"> <li><b>implicit</b>—Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC-class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level.</li> <li><b>explicit <i>precedence-level</i></b>—Specifies a precedence level from 0 to 7 for the traffic to be bumped to.</li> <li><b>traffic</b>—Specifies that the VC or PVC accepts bumped traffic (the default condition). The <b>no</b> form of this command stipulates that the VC or PVC does not accept any bumped traffic.</li> </ul>
<p><b>Step 7</b></p> <pre>protect {group   vc}</pre> <p><b>Example:</b> Router(config-vc-class)# protect vc</p>	<p>Configures a VC class with protected group or protected VC status for application to a VC bundle member.</p> <ul style="list-style-type: none"> <li>This command makes a bundle member part of the protected group of a bundle or a protected VC in a bundle.</li> <li><b>group</b>—Configures the VC or PVC bundle member as part of the protected group of the bundle.</li> <li><b>vc</b>—Configures the VC or PVC member as individually protected.</li> </ul>
<p><b>Step 8</b></p> <pre>exit</pre> <p><b>Example:</b> Router(config-vc-class)# exit</p>	<p>Exits the current configuration mode.</p> <ul style="list-style-type: none"> <li>Continue entering <b>exit</b> at the prompt to exit each configuration mode.</li> </ul>

## Attaching a Class to a Bundle

Perform this task to attach a VC class containing bundle-level configuration commands to a bundle. Enter the **bundle** command in global configuration mode to enter bundle configuration mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [*.subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **bundle** *bundle-name*
5. **class-bundle** *vc-class-name*
6. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface atm</b> <i>interface-number</i> [ <i>.subinterface-number</i> { <b>mpls</b>   <b>multipoint</b>   <b>point-to-point</b> }]  <b>Example:</b> Router(config)# interface atm 0/0/3	Configures an ATM interface and enters interface configuration mode.
Step 4	<b>bundle</b> <i>bundle-name</i>  <b>Example:</b> Router(config-if)# bundle new-york	Creates or modifies a bundle and enters bundle configuration mode. <ul style="list-style-type: none"><li>• <i>bundle-name</i>—Specifies the name of the bundle to be created. Name is limited to 16 characters.</li></ul>
Step 5	<b>class-bundle</b> <i>vc-class-name</i>  <b>Example:</b> Router(config-if-atm-bundle)# class-bundle class1	Configures a bundle with the bundle-level commands contained in the specified VC class.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-if-atm-bundle)# exit	Exits the current configuration mode. <ul style="list-style-type: none"><li>• Continue entering <b>exit</b> at the prompt to exit each configuration mode.</li></ul>

## Configuring a VC Bundle at the Subinterface Level

Perform this task to configure a bundle at the subinterface configuration level. The bundle submode is activated by entering the **bundle** command. This mode is similar to the VC mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [*.subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **bundle** *bundle-name*
5. **encapsulation** [**aal5mux** | **aal5snap**]
6. **protocol** *protocol* {*protocol-address* | **inarp**} [[**no**] **broadcast**]
7. **class** *class-name*
8. **pvc-bundle** *pvc-name* [**vpi**]/[**vci**]
9. **ubr** *pcr*
10. **vbr-nrt** *pcr scr* [*mbs*]
11. **exit**
12. **oam-bundle** [**manage**] [*frequency*]
13. **oam retry** [*up-count*] [*down-count*] [*retry-frequency*]
14. **inarp** [*minutes*]
15. **broadcast**
16. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface atm</b> <i>interface-number</i> [ <i>.subinterface-number</i> { <b>mpls</b>   <b>multipoint</b>   <b>point-to-point</b> }]  <b>Example:</b> Router(config)# interface atm 0/0/3	Configures an ATM interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<b>bundle</b> <i>bundle-name</i>  <b>Example:</b> Router(config-if)# bundle new-york	Creates or modifies a bundle and enters bundle configuration mode. <ul style="list-style-type: none"> <li><i>bundle-name</i>—Specifies the name of the bundle to be created. Name is limited to 16 characters.</li> </ul>
Step 5	<b>encapsulation</b> [ <b>aal5mux</b>   <b>aal5snap</b> ]  <b>Example:</b> Router(config-atm-bundle)# encapsulation aal5snap	Configures the AAL and encapsulation type for every VC in the bundle. <ul style="list-style-type: none"> <li><b>aal5mux</b>—AAL and encapsulation type for multiplex (MUX) type VCs. A protocol must be specified when using this encapsulation type.</li> <li><b>aal5snap</b>—AAL and encapsulation type that supports Inverse ARP.</li> </ul>
Step 6	<b>protocol</b> <i>protocol</i> [ <i>protocol-address</i>   <b>inarp</b> ] [[ <b>no</b> ] <b>broadcast</b> ]  <b>Example:</b> Router(config-atm-bundle)# protocol clns 10.0000.0000.0000.3333.00 broadcast	Configures a static map (the map statement for the bundle) for an ATM PVC, SVC, or VC class. <ul style="list-style-type: none"> <li><i>protocol</i>—Networking protocol.</li> <li><i>protocol-address</i>—Destination address that is being mapped to a PVC.</li> <li><b>inarp</b>—(Valid only for IP and IPX protocols on PVCs) Enables Inverse ARP on an ATM PVC. If you specify a protocol address instead of the <b>inarp</b> keyword, Inverse ARP is automatically disabled for that protocol.</li> <li><b>[no] broadcast</b>—Indicates that this map entry is used when the corresponding protocol sends broadcast packets to the interface.</li> </ul> <p><b>Note</b> Pseudobroadcasting is supported. The <b>broadcast</b> keyword of the <b>protocol</b> command takes precedence if you previously configured the <b>broadcast</b> command on the ATM PVC or SVC.</p>
Step 7	<b>class</b> <i>class-name</i>  <b>Example:</b> Router(config-atm-bundle)# class control-class	Attaches a named VC class to this bundle.

	Command or Action	Purpose
Step 8	<p><b>pvc-bundle</b> <i>pvc-name</i> [<b>vpi</b>/][<b>vci</b>]</p> <p><b>Example:</b> Router(config-if-atm-bundle)# pvc-bundle ny-control 207</p>	<p>Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure VC specific parameters.</p> <ul style="list-style-type: none"> <li>The VC is created upon exiting the mode.</li> <li><b>vpi</b>—ATM network virtual path identifier (VPI) for this PVC. The absence of the slash mark (/) and a VPI value defaults the value to 0. The <b>vpi</b> and <b>vci</b> keywords cannot both be set to 0.</li> <li><b>vci</b>—ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the <b>atm vc-per-vp</b> command.</li> </ul> <p><b>Note</b> The <b>pvc-bundle</b> command is used instead of the <b>pvc</b> command to avoid the ambiguity between this command and the interface <b>pvc</b> command.</p>
Step 9	<p><b>ubr</b> <i>pcr</i></p> <p><b>Example:</b> Router(config-if-atm-member)# ubr 10000</p>	<p>Configures UBR QoS and specifies the output PCR for the VC bundle member.</p>
Step 10	<p><b>vbr-nrt</b> <i>pcr scr [mbs]</i></p> <p><b>Example:</b> Router(config-if-atm-member)# vbr-nrt 20000 10000 32</p>	<p>Configures VBR-nrt QoS with a PCR, an SCR, and MBS.</p>
Step 11	<p><b>exit</b></p> <p><b>Example:</b> Router(config-if-atm-member)# exit</p>	<p>Exits bundle-VC configuration mode and returns to bundle configuration mode.</p>
Step 12	<p><b>oam-bundle</b> [<b>manage</b>] [<i>frequency</i>]</p> <p><b>Example:</b> Router(config-if-atm-member)# oam-bundle manage 6</p>	<p>Enables OAM for every VC in the bundle.</p> <ul style="list-style-type: none"> <li><b>manage</b>—Enables OAM management. If this keyword is omitted, loopback cells are sent, but the bundle is not managed.</li> <li><i>frequency</i>—Seconds between transmitted OAM loopback cells. Default is 10 seconds.</li> </ul>
Step 13	<p><b>oam retry</b> [<i>up-count</i>] [<i>down-count</i>] [<i>retry-frequency</i>]</p> <p><b>Example:</b> Router(config-if-atm-member)# oam retry 5 3 10</p>	<p>Configures OAM parameters for every VC in the bundle.</p> <ul style="list-style-type: none"> <li><i>up-count</i>—Consecutive end-to-end F5 OAM loopback cell responses that must be received to change a connection state to up. Default is 3.</li> <li><i>down-count</i>—Consecutive end-to-end F5 OAM loopback cell responses that are not received to change a PVC state to down. Default is 5.</li> <li><i>retry-frequency</i>—Frequency (in seconds) that end-to-end F5 OAM loopback cells are transmitted when a change in the up/down state is being verified. Default is 1 second.</li> </ul>

	Command or Action	Purpose
Step 14	<b>inarp</b> <i>[minutes]</i>  <b>Example:</b> Router(config-if-atm-member)# inarp 1	Configures the Inverse ARP time period. <ul style="list-style-type: none"><li>• Default is 15 minutes.</li></ul>
Step 15	<b>broadcast</b>  <b>Example:</b> Router(config-if-atm-member)# broadcast	Enables broadcast forwarding on this bundle.
Step 16	<b>exit</b>  <b>Example:</b> Router(config-if-atm-member)# exit	Exits the current configuration mode. <ul style="list-style-type: none"><li>• Continue entering <b>exit</b> at the prompt to exit each configuration mode.</li></ul>

## Assigning VC and Bundle Attributes

The **pvc-bundle** command activates the bundle-VC configuration mode, in which specific VC and bundle member attributes can be assigned.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm** *interface-number* [*.subinterface-number* {**mpls** | **multipoint** | **point-to-point**}]
4. **bundle** *bundle-name*
5. **pvc-bundle** *pvc-name* [**vpi**/][**vci**]
6. **class** *class-name*
7. **ubr** *pcr*
8. **vbr-nrt** *pcr scr* [*mbs*]
9. **mpls experimental** [**other** | *range*]
10. **bump** {**implicit** | **explicit** *precedence-level* | *traffic*}
11. **protect** {**group** | **vc**}
12. **exit**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>interface atm</b> <i>interface-number</i> [.subinterface-number {<b>mpls</b>   <b>multipoint</b>   <b>point-to-point</b>}]</p> <p><b>Example:</b> Router(config)# interface atm 0/0/3</p>	<p>Configures an ATM interface and enters interface configuration mode.</p>
Step 4	<p><b>bundle</b> <i>bundle-name</i></p> <p><b>Example:</b> Router(config-if)# bundle new-york</p>	<p>Creates or modifies a bundle and enters bundle configuration mode.</p>
Step 5	<p><b>pvc-bundle</b> <i>pvc-name</i> [<b>vpi</b>/][<b>vci</b>]</p> <p><b>Example:</b> Router(config-if-atm-bundle)# pvc-bundle ny-control 207</p>	<p>Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure VC specific parameters.</p> <ul style="list-style-type: none"> <li>The VC is created upon exiting the mode.</li> <li><b>vpi</b>—ATM network virtual path identifier (VPI) for this PVC. The absence of the slash mark (/) and a VPI value defaults the value to 0. The <b>vpi</b> and <b>vci</b> keywords cannot both be set to 0.</li> <li><b>vci</b>—ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the <b>atm vc-per-vp</b> command.</li> </ul> <p><b>Note</b> The <b>pvc-bundle</b> command is used instead of the <b>pvc</b> command to avoid the ambiguity between this command and the interface <b>pvc</b> command.</p>
Step 6	<p><b>class</b> <i>class-name</i></p> <p><b>Example:</b> Router(config-if-atm-member)# class control-class</p>	<p>Attaches a VC class to this VC.</p>
Step 7	<p><b>ubr</b> <i>pcr</i></p> <p><b>Example:</b> Router(config-if-atm-member)# ubr 10000</p>	<p>Configures UBR QoS and specifies the output PCR for the VC bundle member.</p>

	Command or Action	Purpose
Step 8	<b>vbr-nrt</b> <i>pcr scr [mbs]</i>  <b>Example:</b> Router(config-if-atm-member)# vbr-nrt 20000 10000 32	Configures VBR-nrt QoS with a PCR, an SCR, and MBS.
Step 9	<b>mpls experimental</b> [ <i>other</i>   <i>range</i> ]  <b>Example:</b> Router(config-if-atm-member)# mpls experimental 7	Defines the experimental levels for packets to be forwarded on this PVC. <ul style="list-style-type: none"> <li>• <b>other</b>—Any precedence level from 0 to 7 not explicitly configured.</li> <li>• <b>range</b>—An MPLS EXP level specified as a number or a range of numbers. Ranges can be expressed with a hyphen (2-5, for example), and numbers and ranges can be expressed in groups separated by commas; 1, 3, 5-7, for example.</li> </ul>
Step 10	<b>bump</b> { <i>implicit</i>   <i>explicit precedence-level</i>   <i>traffic</i> }  <b>Example:</b> Router(config-if-atm-member)# bump explicit 7	Specifies the bumping rule for the VC. <ul style="list-style-type: none"> <li>• <b>implicit</b>—Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level.</li> <li>• <b>explicit precedence-level</b>—Specifies a precedence level from 0 to 7 for the traffic to be bumped to.</li> <li>• <b>traffic</b>—Specifies that the VC or PVC accepts bumped traffic (the default condition). The <b>no</b> form of this command stipulates that the VC or PVC does not accept any bumped traffic.</li> </ul>
Step 11	<b>protect</b> { <i>group</i>   <i>vc</i> }  <b>Example:</b> Router(config-if-atm-member)# protect vc	Configures a VC class with protected group or protected VC status for application to a VC bundle member. <ul style="list-style-type: none"> <li>• This command makes a bundle member part of the protected group of a bundle or a protected VC in a bundle.</li> <li>• <b>group</b>—Configures the VC or PVC bundle member as part of the protected group of the bundle.</li> <li>• <b>vc</b>—Configures the VC or PVC member as individually protected.</li> </ul>
Step 12	<b>exit</b>  <b>Example:</b> Router(config-if-atm-member)# exit	Exits the current configuration mode. <ul style="list-style-type: none"> <li>• Continue entering <b>exit</b> at the prompt to exit each configuration mode.</li> </ul>

# Verifying ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection Configuration

Use the commands in the following steps as needed, to verify configurations for the ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection feature.

## SUMMARY STEPS

1. **enable**
2. **debug atm bundle adjacency events**
3. **debug atm bundle error**
4. **debug atm bundle events**
5. **debug atm bundle inarp**
6. **show atm bundle** *[bundle-name]*
7. **show mpls forwarding-table** [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>debug atm bundle adjacency events</b>  <b>Example:</b> Router# debug atm bundle adjacency	Displays information about adjacency events such as addition, removal, and update of adjacencies for the bundle.
Step 3	<b>debug atm bundle error</b>  <b>Example:</b> Router# debug atm bundle error	Displays debug messages for PVC bundle errors.
Step 4	<b>debug atm bundle events</b>  <b>Example:</b> Router# debug atm bundle event	Displays bundle events such as when VC bumping occurs, when the bundle goes up or down, and so on.
Step 5	<b>debug atm bundle inarp</b>  <b>Example:</b> Router# debug atm bundle inarp	Displays information about Inverse ARP events and errors on the bundle.

	Command or Action	Purpose
Step 6	<b>show atm bundle</b> [ <i>bundle-name</i> ]  <b>Example:</b> Router# show atm bundle new-york	Displays the bundle attributes assigned to each VC member and the current working status of the VC members.
Step 7	<b>show mpls forwarding-table</b> [{ <i>network</i> { <i>mask</i>   <i>length</i> }   <i>labels</i> <i>label</i> [- <i>label</i> ]   <b>interface</b> <i>interface</i>   <i>next-hop</i> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ]}] [ <i>detail</i> ]  <b>Example:</b> Router# show mpls forwarding-table detail	Displays the contents of the MPLS FIB.

## Configuration Examples for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

This section provides the following configuration examples:

- [Configuring MPLS: Example, page 22](#)
- [Defining ATM VC Classes and Parameters: Example, page 22](#)
- [Associating an ATM VC Bundle with the Interface: Example, page 23](#)
- [Creating a VC Class: Example, page 24](#)

### Configuring MPLS: Example

The following example shows how to configure MPLS:

```
ip cef
mpls ldp advertise-labels
!
interface atm 0/0/3
 ip address 10.13.11.3 255.255.0.0
 mpls ip
 bundle bundle1
```

### Defining ATM VC Classes and Parameters: Example

In the following example, VC classes are defined with parameters applicable to individual VCs in the bundle. Each VC class is preceded by a description of how it will be used.

```
! The following commands define the bundle class. Any bundle that uses this class will
! have AAL5snap encapsulation, broadcast on, use of Inverse ARP to resolve IP addresses,
! and OAM enabled at the bundle class level in the inheritance chain.
! This router uses IS-IS as an IP routing protocol.
!
router isis
 net 10.0000.0000.0000.1111.00
!
vc-class atm bundle-class
 encapsulation aal5snap
```

```

broadcast
protocol ip inarp
oam-bundle manage 3
oam 4 3 10
!
! The following VC class defines the parameters applicable to an individual VC
! in a bundle. The control-class carries precedence 7 traffic and it takes the
! bundle down when it is down. It uses the implicit bumping rule.
! The QoS is set to VBR-nrt.
!
vc-class atm control-class
mpls experimental 7
protect vc
vbr-nrt 10000 5000 32
!
! The following VC class defines a premium class that carries precedence level 6 and 5
! traffic. It does not allow other traffic to be bumped onto it. The VC will choose
! precedence 7 VC as the alternate VC for its traffic when it goes down, and it belongs
! to the protected group of the bundle. The QoS type is VBR-nrt.
!
vc-class atm premium-class
mpls experimental 6-5
no bump traffic
protect group
bump explicit 7
vbr-nrt 20000 10000 32
!
! The following VC class defines a priority class that carries precedence levels
! 4 through 2 traffic, uses the implicit bumping rule, allows bumped traffic,
! and belongs to the protected group of the bundle. The QoS type is UBR+.
!
vc-class atm priority-class
mpls experimental 4-2
protect group
ubr+ 10000 3000
!
! The following VC class defines a basic-class that carries the traffic of the precedence
! levels not specified in the profile; it is part of a protected group.
! The QoS type is UBR.
!
vc-class atm basic-class
mpls experimental other
protect group
ubr 10000

```

## Associating an ATM VC Bundle with the Interface: Example

The following interface has one bundle, new-york, for connecting to three neighbors: new-york, san-francisco, and los-angeles. The new-york and san-francisco bundles have four members and los-angeles has three members.

```

interface atm 1/0.1 multipoint
ip address 10.0.0.1 255.255.255.0
ip router isis
bundle new-york
!
! The following commands enable IP and OSI traffic flows in the bundle. The protocol ip
! command takes precedence over the protocol ip inarp command in the bundle class,
! according to the inheritance rule. The protocol clns command is configured so IP routing
! can be integrated. The OSI routing packets will go on the highest precedence VC in the
! bundle, while the OSI data packets, if any, will use the lowest precedence VC in the

```

```

! bundle. Other protocols such as IPX or AppleTalk, if configured, would always use the
! lowest precedence VC in the bundle.
  protocol ip 10.10.1.2 broadcast
  protocol clns 49.0000.0000.0000.2222.00 broadcast
  class bundle-class
!
! The following commands show how to configure the PVC bundles, including adding a VC
! to a bundle as a member.
  pvc-bundle ny-control 207
    class control-class
  pvc-bundle ny-premium 206
    class premium-class
  pvc-bundle ny-priority 204
    class priority-class
  pvc-bundle ny-basic 201
    class basic-class
bundle san-francisco
  protocol clns 49.0000.0000.0000.3333.00 broadcast
  inarp 1
  class bundle-class
  pvc-bundle sf-control 307
    class control-class
  pvc-bundle sf-premium 306
    class premium-class
  pvc-bundle sf-priority 304
    class priority-class
  pvc-bundle sf-basic 301
    class basic-class
bundle los-angeles
  protocol ip 1.1.1.4 broadcast
  protocol clns 49.0000.0000.0000.4444.00 broadcast
  inarp 1
  class bundle-class
  pvc-bundle la-high 407
    precedence 7-5
    protect vc
    class premium-class
  pvc-bundle la-mid 404
    precedence 4-2
    protect group
    class priority-class
  pvc-bundle la-low 401
    precedence other
    protect group
    class basic-class
!
The following commands configure PVC la-other as a standalone VC that does not belong to
any of the bundles.
!
  pvc la-other 400
    no protocol ip inarp
    broadcast

```

## Creating a VC Class: Example

In the following example, a class called class1 is created and then applied to the bundle called bundle1:

```

! The following commands create the class class1:
vc-class atm class1
  encapsulation aal5snap
  broadcast
  protocol ip inarp

```

```
oam-bundle manage 3
oam 4 3 10
!
! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
class-bundle class1
```

With hierarchy precedence rules taken into account, VCs belonging to the bundle named bundle1 will be characterized by these parameters: AAL5SNAP (RFC1483 bridging) encapsulation, broadcast on, use of Inverse ARP to resolve IP addresses, and OAM enabled.

## Additional References

The following sections provide references related to the ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection feature.

### Related Documents

Related Topic	Document Title
QoS Overview	<a href="#">Cisco IOS Quality of Service Overview</a>
QoS Commands	<a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>
Configuring ATM	<a href="#">Configuring ATM</a>
SVC bundles	<a href="#">IP to ATM SVC Bundles for Class of Service (CoS) Mapping</a>
ATM VC bundle management on Cisco 12000 Series Internet Routers	<a href="#">ATM VC Bundle Management on Cisco 12000 Series 8-Port OC-3 STM-1 ATM Line Cards</a>

### Standards

Standards	Title
None	—

### MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFCs	Title
None	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>



# Feature Information for ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for ATM PVC Bundle Enhancement — MPLS EXP-Based PVC Selection

Feature Name	Releases	Feature Information
ATM PVC Bundle Enhancement — MPLS EXP-Based PVC Selection	12.2(8)T 12.0(23)S 12.0(29)S 12.2(33)SRC	<p>In Cisco IOS Release 12.2(8)T, this feature was introduced.</p> <p>In Cisco IOS Release 12.0(23)S, this feature was made available on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers.</p> <p>This feature was integrated into Cisco IOS Release 12.0(29)S.</p> <p>In Cisco IOS Release 12.2(33)SRC, support was added for the Cisco 7200 series router.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection, page 2</a></li> <li>• <a href="#">How to Configure ATM PVC Bundle Enhancement—MPLS EXP-Based PVC Selection, page 6</a></li> </ul> <p>The following commands were introduced or modified: <b>mpls experimental, show mpls forwarding-table.</b></p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2006-2009 Cisco Systems, Inc. All rights reserved.



## **MPLS Label Distribution Protocol**





# MPLS Label Distribution Protocol (LDP)

---

**First Published: January 1, 1999**

**Last Updated: May 1, 2008**

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding in an MPLS network. This module explains the concepts related to MPLS LDP and describes how to configure MPLS LDP in a network.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS Label Distribution Protocol](#)” section on [page 27](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS LDP, page 2](#)
- [Information About MPLS LDP, page 2](#)
- [Information About MPLS LDP, page 2](#)
- [How to Configure MPLS LDP, page 5](#)
- [MPLS LDP Configuration Examples, page 20](#)
- [Command Reference, page 26](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

# Prerequisites for MPLS LDP

Label switching on a router requires that Cisco Express Forwarding (CEF) be enabled on that router.

## Information About MPLS LDP

To configure MPLS LDP, you should understand the following concepts:

- [Introduction to MPLS LDP, page 2](#)
- [MPLS LDP Functional Overview, page 2](#)
- [LDP and TDP Support, page 2](#)
- [Introduction to LDP Sessions, page 3](#)
- [Introduction to LDP Label Bindings, Label Spaces, and LDP Identifiers, page 4](#)

## Introduction to MPLS LDP

MPLS LDP provides the means for LSRs to request, distribute, and release label prefix binding information to peer routers in a network. LDP enables LSRs to discover potential peers and to establish LDP sessions with those peers for the purpose of exchanging label binding information.

MPLS LDP enables one LSR to inform another LSR of the label bindings it has made. Once a pair of routers communicate the LDP parameters, they establish a label-switched path (LSP). MPLS LDP enables LSRs to distribute labels along normally routed paths to support MPLS forwarding. This method of label distribution is also called hop-by-hop forwarding. With IP forwarding, when a packet arrives at a router the router looks at the destination address in the IP header, performs a route lookup, and forwards the packet to the next hop. With MPLS forwarding, when a packet arrives at a router the router looks at the incoming label, looks up the label in a table, and then forwards the packet to the next hop. MPLS LDP is useful for applications that require hop-by-hop forwarding, such as MPLS VPNs.

## MPLS LDP Functional Overview

Cisco MPLS LDP provides the building blocks for MPLS-enabled applications, such as MPS Virtual Private Networks (VPNs).

LDP provides a standard methodology for hop-by-hop, or dynamic label, distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying Interior Gateway Protocol (IGP) routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward label traffic across an MPLS backbone to particular destinations. These capabilities enable service providers to implement MPLS-based IP VPNs and IP+ATM services across multivendor MPLS networks.

## LDP and TDP Support

LDP supersedes Tag Distribution Protocol (TDP). See [Table 1](#) for information about LDP and TDP support in Cisco IOS releases.

Use caution when upgrading the image on a router that uses TDP. Ensure that the TDP sessions are established when the new image is loaded. You can accomplish this by issuing the global configuration command **mpls label protocol tdp**. Issue this command and save it to the startup configuration before loading the new image. Alternatively, you can enter the command and save the running configuration immediately after loading the new image.

**Table 1** *LDP and TDP Support*

Train and Release	LDP/TDP Support
12.0S Train	<ul style="list-style-type: none"> <li>TDP is enabled by default.</li> <li>Cisco IOS Release 12.0(29)S and earlier releases: TDP is supported for LDP features.</li> <li>Cisco IOS Release 12.0(30)S and later releases: TDP is not support for LDP features.</li> </ul>
12.2S, SB, and SR Trains	<ul style="list-style-type: none"> <li>LDP is enabled by default.</li> <li>Cisco IOS Release 12.2(25)S and earlier releases: TDP is supported for LDP features.</li> <li>Cisco IOS Releases 12.2(27)SBA, 12.2(27)SRA, 12.2(27)SRB and later releases: TDP is not supported for LDP features.</li> </ul>
12.T/Mainline Trains	<ul style="list-style-type: none"> <li>Cisco IOS Release 12.3(14)T and earlier releases: TDP is enabled by default.</li> <li>Cisco IOS Releases 12.4 and 12.4T and later releases: LDP is enabled by default.</li> <li>Cisco IOS Release 12.3(11)T and earlier releases: TDP is supported for LDP features.</li> <li>Cisco IOS Release 12.3(14)T and later releases: TDP is not support ed for LDP features.</li> </ul>

## Introduction to LDP Sessions

When you enable MPLS LDP, the LSRs send out messages to try to find other LSRs with which they can create LDP sessions. The following sections explain the differences between directly connected LDP sessions and nondirectly connected LDP sessions.

### Directly Connected MPLS LDP Sessions

If an LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP link Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet (multicast). A neighboring LSR may respond to the link Hello message, allowing the two routers to establish an LDP session. This is called basic discovery.

To initiate an LDP session between routers, the routers determine which router will take the active role and which router will take the passive role. The router that takes the active role establishes the LDP TCP connection session and initiates the negotiation of the LDP session parameters. To determine the roles, the two routers compare their transport addresses. The router with the higher IP address takes the active role and establishes the session.

After the LDP TCP connection session is established, the LSRs negotiate the session parameters, including the method of label distribution to be used. Two methods are available:

- Downstream Unsolicited: An LSR advertises label mappings to peers without being asked to.
- Downstream on Demand: An LSR advertises label mappings to a peer only when the peer asks for them.

For information about creating LDP sessions, see the [“Enabling Directly Connected LDP Sessions” section on page 6](#).

## Nondirectly Connected MPLS LDP Sessions

If the LSR is more than one hop from its neighbor, it is nondirectly connected to its neighbor. For these nondirectly connected neighbors, the LSR sends out a targeted Hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The nondirectly connected LSR responds to the Hello message and the two routers begin to establish an LDP session. This is called extended discovery.

An MPLS LDP targeted session is a label distribution session between routers that are not directly connected. When you create an MPLS traffic engineering tunnel interface, you need to establish a label distribution session between the tunnel headend and the tailend routers. You establish nondirectly connected MPLS LDP sessions by enabling the transmission of targeted Hello messages.

You can use the **mpls ldp neighbor targeted** command to set up a targeted session when other means of establishing targeted sessions do not apply, such as configuring **mpls ip** on a traffic engineering (TE) tunnel or configuring Any Transport over MPLS (AToM) virtual circuits (VCs). For example, you can use this command to create a targeted session between directly connected MPLS label switch routers (LSRs) when MPLS label forwarding convergence time is an issue.

The **mpls ldp neighbor targeted** command can improve label convergence time for directly connected neighbor LSRs when the link(s) directly connecting them are down. When the links between the neighbor LSRs are up, both the link and targeted Hellos maintain the LDP session. If the links between the neighbor LSRs go down, the targeted Hellos maintain the session, allowing the LSRs to retain labels learned from each other. When a link directly connecting the LSRs comes back up, the LSRs can immediately reinstall labels for forwarding use without having to reestablish their LDP session and exchange labels.

The exchange of targeted Hello messages between two nondirectly connected neighbors can occur in several ways, including the following:

- Router 1 sends targeted Hello messages carrying a response request to Router 2. Router 2 sends targeted Hello messages in response if its configuration permits. In this situation, Router 1 is considered to be *active* and Router 2 is considered to be *passive*.
- Router 1 and Router 2 both send targeted Hello messages to each other. Both routers are considered to be *active*. Both, one, or neither router can also be *passive*, if they have been configured to respond to requests for targeted Hello messages from each other.

The default behavior of an LSR is to ignore requests from other LSRs that send targeted Hello messages. You can configure an LSR to respond to requests for targeted Hello messages by issuing the **mpls ldp discovery targeted-hello accept** command.

The active LSR mandates the protocol that is used for a targeted session. The passive LSR uses the protocol of the received targeted Hello messages.

For information about creating MPLS LDP targeted sessions, see the [“Establishing Nondirectly Connected MPLS LDP Sessions”](#) section on page 8.

## Introduction to LDP Label Bindings, Label Spaces, and LDP Identifiers

An LDP label binding is an association between a destination prefix and a label. The label used in a label binding is allocated from a set of possible labels called a label space.

LDP supports two types of label spaces:

- Interface-specific—An interface-specific label space uses interface resources for labels. For example, label-controlled ATM (LC-ATM) interfaces use virtual path identifiers/virtual circuit identifiers (VPIs/VCI) for labels. Depending on its configuration, an LDP platform may support zero, one, or more interface-specific label spaces.



- Platform-wide—An LDP platform supports a single platform-wide label space for use by interfaces that can share the same labels. For Cisco platforms, all interface types, except LC-ATM, use the platform-wide label space.

LDP uses a 6-byte quantity called an LDP Identifier (or LDP ID) to name label spaces. The LDP ID is made up of the following components:

- The first four bytes, called the LDP router ID, identify the LSR that owns the label space.
- The last two bytes, called the local label space ID, identify the label space within the LSR. For the platform-wide label space, the last two bytes of the LDP ID are always both 0.

The LDP ID takes the following form:

<LDP router ID> : <local label space ID>

The following are examples of LDP IDs:

- 172.16.0.0:0
- 192.168.0.0:3

The router determines the LDP router ID as follows, if the **mpls ldp router-id** command is not executed,

1. The router examines the IP addresses of all operational interfaces.
2. If these IP addresses include loopback interface addresses, the router selects the largest loopback address as the LDP router ID.
3. Otherwise, the router selects the largest IP address pertaining to an operational interface as the LDP router ID.

The normal (default) method for determining the LDP router ID may result in a router ID that is not usable in certain situations. For example, the router might select an IP address as the LDP router ID that the routing protocol cannot advertise to a neighboring router. The **mpls ldp router-id** command allows you to specify the IP address of an interface as the LDP router ID. Make sure the specified interface is operational so that its IP address can be used as the LDP router ID.

When you issue the **mpls ldp router-id** command without the **force** keyword, the router selects the IP address of the specified interface (provided that the interface is operational) the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is configured.

When you issue the **mpls ldp router-id** command with the **force** keyword, the effect of the **mpls ldp router-id** command depends on the current state of the specified interface:

- If the interface is up (operational) and if its IP address is not currently the LDP router ID, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down (not operational) when the **mpls ldp router-id interface force** command is issued, when the interface transitions to up, the LDP router ID changes to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

## How to Configure MPLS LDP

This section contains the following procedures:

- [Enabling Directly Connected LDP Sessions, page 6](#) (required)

- [Establishing Nondirectly Connected MPLS LDP Sessions, page 8](#) (optional)
- [Saving Configurations: MPLS/Tag Switching Commands, page 11](#) (optional)
- [Specifying the LDP Router ID, page 11](#) (optional)
- [Preserving QoS Settings with MPLS LDP Explicit Null, page 13](#) (optional)
- [Protecting Data Between LDP Peers with MD5 Authentication, page 17](#) (optional)

## Enabling Directly Connected LDP Sessions

This procedure explains how to configure MPLS LDP sessions between two directly connected routers.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls ip`
4. `mpls label protocol {ldp | tdp | both}`
5. `interface type number`
6. `mpls ip`
7. `exit`
8. `exit`
9. `show mpls interfaces [interface] [detail]`
10. `show mpls ldp discovery [all | vrf vpn-name] [detail]`
11. `show mpls ldp neighbor [[vrf vpn-name] [address | interface] [detail] | [all]]`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> <code>Router&gt; enable</code>	
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	<b>Example:</b> <code>Router# configure terminal</code>	
Step 3	<code>mpls ip</code>	Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"><li>• The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li><li>• Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li></ul>
	<b>Example:</b> <code>Router(config)# mpls ip</code>	

	Command or Action	Purpose
<b>Step 4</b>	<pre>mpls label protocol {ldp   tdp   both}</pre> <p><b>Example:</b> Router(config)# mpls label protocol ldp</p>	<p>Configures the use of LDP on all interfaces. LDP is the default.</p> <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>
<b>Step 5</b>	<pre>Router(config)# interface type number</pre> <p><b>Example:</b> Router(config)# interface ethernet3/0</p>	Specifies the interface to be configured and enters interface configuration mode.
<b>Step 6</b>	<pre>mpls ip</pre> <p><b>Example:</b> Router(config-if)# mpls ip</p>	<p>Configures MPLS hop-by-hop forwarding on the interface.</p> <ul style="list-style-type: none"> <li>You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
<b>Step 7</b>	<pre>exit</pre> <p><b>Example:</b> Router(config-if)# exit</p>	Exits interface configuration mode and enters global configuration mode.
<b>Step 8</b>	<pre>exit</pre> <p><b>Example:</b> Router(config)# exit</p>	Exits global configuration mode and enters privileged EXEC mode.
<b>Step 9</b>	<pre>show mpls interfaces [interface] [detail]</pre> <p><b>Example:</b> Router# show mpls interfaces</p>	Verifies that the interfaces have been configured to use LDP, TDP, or both.
<b>Step 10</b>	<pre>show mpls ldp discovery [all   vrf vpn-name] [detail]</pre> <p><b>Example:</b> Router# show mpls ldp discovery</p>	Verifies that the interface is up and is sending Discovery Hello messages.
<b>Step 11</b>	<pre>show mpls ldp neighbor [[vrf vpn-name] [address   interface] [detail]   [all]]</pre> <p><b>Example:</b> Router# show mpls ldp neighbor</p>	Displays the status of LDP sessions.

## Examples

The following **show mpls interfaces** command verifies that interfaces Ethernet 1/0 and 1/1 have been configured to use LDP:

```
Router# show mpls interfaces
```

Interface	IP	Tunnel	BGP	Static	Operational
Ethernet3/0	Yes (ldp)	No	No	No	Yes
Ethernet3/1	Yes	No	No	No	Yes

The following **show mpls ldp discovery** command verifies that the interface is up and is sending LDP Discovery Hello messages (as opposed to TDP Hello messages):

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
 172.16.12.1:0
Discovery Sources:
Interfaces:
  Ethernet3/0 (ldp): xmit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor
```

```
Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.18 - 10.1.1.1.66
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2    10.20.20.1    10.20.10.2
```

For examples on configuring directly connected LDP sessions, see the [“Configuring Directly Connected MPLS LDP Sessions: Example”](#) section on page 20.

## Establishing Nondirectly Connected MPLS LDP Sessions

This section explains how to configure nondirectly connected MPLS LDP sessions, which enable you to establish an LDP session between routers that are not directly connected.

### Prerequisites

- MPLS requires CEF.
- You must configure the routers at both ends of the tunnel to be active or enable one router to be passive with the **mpls ldp discovery targeted-hello accept** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol {ldp | tdp | both}**

5. **interface** *tunnelnumber*
6. **tunnel destination** *ip-address*
7. **mpls ip**
8. **exit**
9. **exit**
10. **show mpls ldp discovery** [**all** | **vrf** *vpn-name*] [**detail**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
Step 4	<b>mpls label protocol</b> { <b>ldp</b>   <b>tdp</b>   <b>both</b> }  <b>Example:</b> Router(config)# mpls label protocol ldp	Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>
Step 5	<b>interface</b> <i>tunnelnumber</i>  <b>Example:</b> Router(config)# interface tunnell	Configures a tunnel interface and enters interface configuration mode.
Step 6	<b>tunnel destination</b> <i>ip-address</i>  <b>Example:</b> Router(config-if)# tunnel destination 172.16.1.1	Assigns an IP address to the tunnel interface.
Step 7	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding on the interface. <ul style="list-style-type: none"> <li>You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>

	Command or Action	Purpose
Step 8	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 9	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 10	<b>show mpls ldp discovery</b> [all   vrf vpn-name] [detail]  <b>Example:</b> Router# show mpls ldp discovery	Verifies that the interface is up and is sending Discovery Hello messages.

## Example

The following example shows the output of the **show mpls ldp discovery** command for a nondirectly connected LDP session.

```
Router# show mpls ldp discovery

Local LDP Identifier:
    172.16.0.0:0
Discovery Sources:
Interfaces:
    POS2/0 (ldp): xmit/recv
        LDP Id: 172.31.255.255:0
    Tunnell (ldp): Targeted -> 192.168.255.255
Targeted Hellos:
    172.16.0.0 -> 192.168.255.255 (ldp): active, xmit/recv
        LDP Id: 192.168.255.255:0
    172.16.0.0 -> 192.168.0.0 (tdp): passive, xmit/recv
        TDP Id: 192.168.0.0:0
```

This command output indicates that:

- The local LSR (172.16.0.0) sent LDP link Hello messages on interface POS2/0 and discovered neighbor 172.31.255.255.
- The local LSR sent LDP targeted Hello messages associated with interface Tunnell1 to target 192.168.255.255. The LSR was configured to use LDP.
- The local LSR is active for targeted discovery activity with 192.168.255.255; this means that the targeted Hello messages it sends to 192.168.255.255 carry a response request. The local LSR was configured to have an LDP session with the nondirectly connected LSR 192.168.255.255.
- The local LSR is not passive from the discovery activity with 192.168.255.255 for one of the following reasons:
  - The targeted Hello messages it receives from 192.168.255.255 do not carry a response request.
  - The local LSR has not been configured to respond to such requests.
- The local LSR sent TDP directed Hello messages to the target LSR 192.168.0.0. This LSR uses TDP because the Hello messages received from the target LSR 192.168.0.0 were TDP directed Hello messages.

- The local LSR is passive in discovery activity with LSR 192.168.0.0. This means that the directed Hello messages it receives from LSR 192.168.0.0 carry a response request and that the local LSR has been configured with the **mpls ldp discovery targeted-hello accept** command to respond to such requests from LSR 192.168.0.0.
- The local LSR is not active in discovery activity with LSR 192.168.0.0, because no application that requires an LDP session with LSR 192.168.0.0 has been configured on the local LSR.

For examples of configuring LDP targeted sessions, see the [“Establishing Nondirectly Connected MPLS LDP Sessions: Example”](#) section on page 22.

## Saving Configurations: MPLS/Tag Switching Commands

In releases of Cisco IOS software prior to 12.4(2)T, some MPLS commands had both a tag-switching version and an MPLS version. For example, the two commands **tag-switching ip** and **mpls ip** were the same. To support backward compatibility, the tag-switching form of the command was written to the saved configuration.

Starting in Cisco IOS Release 12.4(2)T, the MPLS form of the command is written to the saved configuration.

For example, if an ATM interface is configured using the following commands, which have both a tag-switching form and an MPLS form:

```
Router(config)# interface ATM3/0
Router(config-if)# ip unnumbered Loopback0
router(config-if)# tag-switching ip
Router(config-if)# mpls label protocol ldp
```

After you enter these commands and save this configuration or display the running configuration with the **show running** command, the commands saved or displayed appear as follows:

```
interface ATM3/0
ip unnumbered Loopback0
mpls ip
mpls label protocol ldp
```

## Specifying the LDP Router ID

The **mpls ldp router-id** command allows you to establish the IP address of an interface as the LDP router ID.

The following steps describe the normal process for determining the LDP router ID:

1. The router considers all the IP addresses of all operational interfaces.
2. If these addresses include loopback interface addresses, the router selects the largest loopback address. Configuring a loopback address helps ensure a stable LDP ID for the router, because the state of loopback addresses does not change. However, configuring a loopback interface and IP address on each router is not required.

The loopback IP address does not become the router ID of the local LDP ID under the following circumstances:

- If the loopback interface has been explicitly shut down.
- If the **mpls ldp router-id** command specifies that a different interface should be used as the LDP router ID.

If you use a loopback interface, make sure that the IP address for the loopback interface is configured with a /32 network mask. In addition, make sure that the routing protocol in use is configured to advertise the corresponding /32 network.

3. Otherwise, the router selects the largest interface address.

The router might select a router ID that is not usable in certain situations. For example, the router might select an IP address that the routing protocol cannot advertise to a neighboring router.

The router implements the router ID the next time it is necessary to select an LDP router ID. The effect of the command is delayed until the next time it is necessary to select an LDP router ID, which is typically the next time the interface is shut down or the address is deconfigured.

If you use the **force** keyword with the **mpls ldp router-id** command, the router ID takes effect more quickly. However, implementing the router ID depends on the current state of the specified interface:

- If the interface is up (operational) and its IP address is not currently the LDP router ID, the LDP router ID is forcibly changed to the IP address of the interface. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.
- If the interface is down, the LDP router ID is forcibly changed to the IP address of the interface when the interface transitions to up. This forced change in the LDP router ID tears down any existing LDP sessions, releases label bindings learned via the LDP sessions, and interrupts MPLS forwarding activity associated with the bindings.

Prerequisites

Make sure the specified interface is operational before assigning it as the LDP router ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol {ldp | tdp | both}**
5. **mpls ldp router-id interface [force]**
6. **exit**
7. **show mpls ldp discovery [all | detail |vrf vpn-name]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	



	Command or Action	Purpose
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
Step 4	<b>mpls label protocol {ldp   tdp   both}</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>
Step 5	<b>mpls ldp router-id interface [force]</b>  <b>Example:</b> Router(config)# mpls ldp router-id pos2/0/0	Specifies the preferred interface for determining the LDP router ID.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 7	<b>show mpls ldp discovery [all   detail   vrf vpn-name]</b>  <b>Example:</b> Router# show mpls ldp discovery	Displays the LDP identifier for the local router.

## Example

The following example assigns interface pos2/0/0 as the LDP router ID:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp router-id pos2/0/0 force
```

The following example displays the LDP router ID (10.15.15.15):

```
Router# show mpls ldp discovery

Local LDP Identifier:
 10.15.15.15:0
Discovery Sources:
 Interfaces:
   Ethernet4 (ldp): xmit/recv
     LDP Id: 10.14.14.14:0
```

## Preserving QoS Settings with MPLS LDP Explicit Null

Normally, LDP advertises an Implicit Null label for directly connected routes. The Implicit Null label causes the second last (penultimate) label switched router (LSR) to remove the MPLS header from the packet. In this case, the penultimate LSR and the last LSR do not have access to the quality of service (QoS) values that the packet carried before the MPLS header was removed. To preserve the QoS values, you can configure the LSR to advertise an explicit NULL label (a label value of zero). The LSR at the penultimate hop forwards MPLS packets with a NULL label instead of forwarding IP packets.



Note

An explicit NULL label is not needed when the penultimate hop receives MPLS packets with a label stack that contains at least two labels and penultimate hop popping is performed. In that case, the inner label can still carry the QoS value needed by the penultimate and edge LSR to implement their QoS policy.

When you issue the **mpls ldp explicit-null** command, Explicit Null is advertised in place of Implicit Null for directly connected prefixes.

SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **mpls ip**
- 4. **mpls label protocol {ldp | tdp | both}**
- 5. **interface** *type number*
- 6. **mpls ip**
- 7. **exit**
- 8. **mpls ldp explicit-null** [**for** *prefix-acl* | **to** *peer-acl* | **for** *prefix-acl to peer-acl*]
- 9. **exit**
- 10. **show mpls forwarding-table** [*network {mask | length}* | **labels** *label* [- *label*] | **interface** *interface* | *next-hop address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vpn-name*] [**detail**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
Step 4	<b>mpls label protocol {ldp   tdp   both}</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>
Step 5	<b>interface type number</b>  <b>Example:</b> Router(config)# interface atm2/0	Specifies the interface to be configured and enters interface configuration mode.
Step 6	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding on the interface. <ul style="list-style-type: none"> <li>You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and enters global configuration mode.
Step 8	<b>mpls ldp explicit-null [for prefix-acl   to peer-acl   for prefix-acl to peer-acl]</b>  <b>Example:</b> Router(config)# mpls ldp explicit-null	Advertises an Explicit Null label in situations where it would normally advertise an Implicit Null label.
Step 9	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and enter privileged EXEC mode.
Step 10	<b>show mpls forwarding-table [network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]] [vrf vpn-name] [detail]</b>  <b>Example:</b> Router# show mpls forwarding-table	Verifies that MPLS packets are forwarded with an explicit-null label (value of 0).

## Examples

Enabling explicit-null on an egress LSR causes that LSR to advertise the explicit-null label to all adjacent MPLS routers.

```
Router# configure terminal
```

```
Router(config)# mpls ldp explicit-null
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that MPLS packets are forwarded with an explicit-null label (value of 0). In the following example, the second column shows that entries have outgoing labels of 0, where once they were marked “Pop label”.

```
Router# show mpls forwarding-table
```

Local label	Outgoing label or VC	Prefix or Tunnel Id	Bytes label switched	Outgoing interface	Next Hop
19	Pop tag	10.12.12.12/32	0	Fa2/1/0	172.16.0.1
22	0	10.14.14.14/32	0	Fa2/0/0	192.168.0.2
23	0	172.24.24.24/32	0	Fa2/0/0	192.168.0.2
24	0	192.168.0.0/8	0	Fa2/0/0	192.168.0.2
25	0	10.15.15.15/32	0	Fa2/0/0	192.168.0.2
26	0	172.16.0.0/8	0	Fa2/0/0	192.168.0.2
27	25	10.16.16.16/32	0	Fa2/0/0	192.168.0.22
28	0	10.34.34.34/32	0	Fa2/0/0	192.168.0.2

Enabling explicit-null and specifying the **for** keyword with a standard access control list (ACL) changes all adjacent MPLS routers' tables to swap an explicit-null label for only those entries specified in the access-list. In the following example, an access-list is created that contains the 10.24.24.24 entry. Explicit null is configured and the access list is specified.

```
Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 24 permit host 10.24.24.24
Router(config)# mpls ldp explicit-null for 24
```

If you issue the **show mpls forwarding-table** command on an adjacent router, the output shows that the only the outgoing labels for the addresses specified (172.24.24.24/32) change from Pop label to 0. All other Pop label outgoing labels remain the same.

```
Router# show mpls forwarding-table
```

Local label	Outgoing label or VC	Prefix or Tunnel Id	Bytes label switched	Outgoing interface	Next Hop
19	Pop tag	10.12.12.12/32	0	Fa2/1/0	172.16.0.1
22	0	10.14.14.14/32	0	Fa2/0/0	192.168.0.2
23	0	172.24.24.24/32	0	Fa2/0/0	192.168.0.2
24	0	192.168.0.0/8	0	Fa2/0/0	192.168.0.2
25	0	10.15.15.15/32	0	Fa2/0/0	192.168.0.2
26	0	172.16.0.0/8	0	Fa2/0/0	192.168.0.2
27	25	10.16.16.16/32	0	Fa2/0/0	192.168.0.22
28	0	10.34.34.34/32	0	Fa2/0/0	192.168.0.2

Enabling explicit null and adding the **to** keyword and an access list enables you to advertise explicit-null labels to only those adjacent routers specified in the access-list. To advertise explicit-null to a particular router, you must specify the router's LDP ID in the access-list.

In the following example, an access-list contains the 10.15.15.15/32 entry, which is the LDP ID of an adjacent MPLS router. The router that is configured with explicit null advertises explicit-null labels only to that adjacent router.

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
 10.15.15.15:0
Discovery Sources:
  Interfaces:
    Ethernet4 (ldp): xmit/recv
      TDP Id: 10.14.14.14:0
```

```

Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# access-list 15 permit host 10.15.15.15
Router(config)# mpls ldp explicit-null to 15

```

If you issue the **show mpls forwarding-table** command, the output shows that explicit null labels are going only to the router specified in the access list.

```
Router# show mpls forwarding-table
```

Local label	Outgoing label or VC Pop tag	Prefix or Tunnel Id	Bytes label switched	Outgoing interface	Next Hop
19		10.12.12.12/32	0	Fa2/1/0	172.16.0.1
22	0	10.14.14.14/32	0	Fa2/0/0	192.168.0.2
23	0	172.24.24.24/32	0	Fa2/0/0	192.168.0.2
24	0	192.168.0.0/8	0	Fa2/0/0	192.168.0.2
25	0	10.15.15.15/32	0	Fa2/0/0	192.168.0.2
26	0	172.16.0.0/8	0	Fa2/0/0	192.168.0.2
27	25	10.16.16.16/32	0	Fa2/0/0	192.168.0.22
28	0	10.34.34.34/32	0	Fa2/0/0	192.168.0.2

Enabling explicit-null with both the **for** and **to** keywords enables you to specify which routes to advertise with explicit-null labels and to which adjacent routers to advertise these explicit-null labels.

```
Router# show access 15
```

```

Standard IP access list 15
  permit 10.15.15.15 (7 matches)

```

```
Router# show access 24
```

```

Standard IP access list 24
  permit 10.24.24.24 (11 matches)

```

```

Router# configure terminal
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp explicit-null for 24 to 15

```

If you issue the **show mpls forwarding-table** command on the router called 47K-60-4, the output shows that it receives explicit null labels for 10.24.24.24/32.

```
Router# show mpls forwarding-table
```

Local label	Outgoing label or VC	Prefix or Tunnel Id	Bytes label switched	Outgoing interface	Next Hop
17	0 <---	10.24.24.24/32	0	Et4	172.16.0.1
20	Pop tag	172.16.0.0/8	0	Et4	172.16.0.1
21	20	10.12.12.12/32	0	Et4	172.16.0.1
22	16	10.0.0.0/8	0	Et4	172.16.0.1
23	21	10.13.13.13/32	0	Et4	172.16.0.1
25	Pop tag	10.14.14.14/32	0	Et4	172.16.0.1
27	Pop tag	192.168.0.0/8	0	Et4	172.16.0.1
28	25	10.16.16.16/32	0	Et4	172.16.0.1
29	Pop tag	192.168.34.34/32	0	Et4	172.16.0.1

## Protecting Data Between LDP Peers with MD5 Authentication

You can enable authentication between two LDP peers, which verifies each segment sent on the TCP connection between the peers. You must configure authentication on both LDP peers using the same password; otherwise, the peer session is not established.

Authentication uses the Message Digest 5 (MD5) algorithm to verify the integrity of the communication and authenticate the origin of the message.

To enable authentication, issue the **mpls ldp neighbor** command with the **password** keyword. This causes the router to generate an MD5 digest for every segment sent on the TCP connection and check the MD5 digest for every segment received from the TCP connection.

When you configure a password for an LDP neighbor, the router tears down existing LDP sessions and establishes new sessions with the neighbor.

If a router has a password configured for a neighbor, but the neighboring router does not have a password configured, a message such as the following appears on the console who has a password configured while the two routers attempt to establish an LDP session. The LDP session is not established.

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address](11003) to [local router's IP address](646)
```

Similarly, if the two routers have different passwords configured, a message such as the following appears on the console. The LDP session is not established.

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address](11004) to [local router's IP address](646)
```

SUMMARY STEPS

- 1. **enable**
- 2. **configure terminal**
- 3. **mpls ip**
- 4. **mpls label protocol {ldp | tdp | both}**
- 5. **mpls ldp neighbor [vrf vpn-name] ip-address [password [0-7] password-string]**
- 6. **show mpls ldp neighbor [[vrf vpn-name] [address | interface] [detail] | [all]]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Configures MPLS hop-by-hop forwarding globally. <ul style="list-style-type: none"> <li>The <b>mpls ip</b> command is enabled by default; you do not have to specify this command.</li> <li>Globally enabling MPLS forwarding does not enable it on the router interfaces. You must enable MPLS forwarding on the interfaces as well as for the router.</li> </ul>
Step 4	<b>mpls label protocol {ldp   tdp   both}</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Configures the use of LDP on all interfaces. LDP is the default. <ul style="list-style-type: none"> <li>If you set all interfaces globally to LDP, you can override specific interfaces with either the <b>tdp</b> or <b>both</b> keyword by specifying the command in interface configuration mode.</li> </ul>
Step 5	<b>mpls ldp neighbor [vrf vpn-name] ip-address [password [0-7] password-string]</b>  <b>Example:</b> Router(config)# mpls ldp neighbor 172.27.0.15 password onethirty9	Specifies authentication between two LDP peers.
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and enters privileged EXEC mode.
Step 7	<b>show mpls ldp neighbor [[vrf vpn-name] [address   interface] [detail]   [all]]</b>  <b>Example:</b> Router# show mpls ldp neighbor detail	Displays the status of LDP sessions.  If the passwords have been set on both LDP peers and the passwords match, the <b>show mpls ldp neighbor</b> command displays that the LDP session was successfully established.

## Examples

The following example configures a router with the password cisco:

```
Router> enable
Router# configure terminal
Router(config)# mpls ip
Router(config)# mpls label protocol ldp
Router(config)# mpls ldp neighbor 10.1.1.1 password cisco
Router(config)# exit
```

The following example shows that the LDP session between routers was successfully established:

```
Router# show mpls ldp neighbor

Peer LDP Ident: 10.1.1.2:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.1.1.2.11118 - 10.1.1.1.646
State: Oper; Msgs sent/rcvd: 12/11; Downstream
Up time: 00:00:10
LDP discovery sources:
FastEthernet1/0, Src IP addr: 10.20.10.2
Addresses bound to peer LDP Ident:
10.1.1.2    10.20.20.1    10.20.10.2
```

The following **show mpls ldp neighbor detail** command shows that MD5 (shown in bold) is used for the LDP session.

```
Router# show mpls ldp neighbor 10.0.0.21 detail

Peer LDP Ident: 10.0.0.21:0; Local LDP Ident 10.0.0.22:0
TCP connection: 10.0.0.21.646 - 10.0.0.22.14709; MD5 on
State: Oper; Msgs sent/rcvd: 1020/1019; Downstream; Last TIB rev sent 2034
Up time: 00:00:39; UID: 3; Peer Id 1;
LDP discovery sources:
  FastEthernet1/1; Src IP addr: 172.16.1.1
    holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
  10.0.0.21      10.0.38.28      10.88.88.2      172.16.0.1
  172.16.1.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

## MPLS LDP Configuration Examples

This section includes the following configuration examples:

- [Configuring Directly Connected MPLS LDP Sessions: Example, page 20](#)
- [Establishing Nondirectly Connected MPLS LDP Sessions: Example, page 22](#)

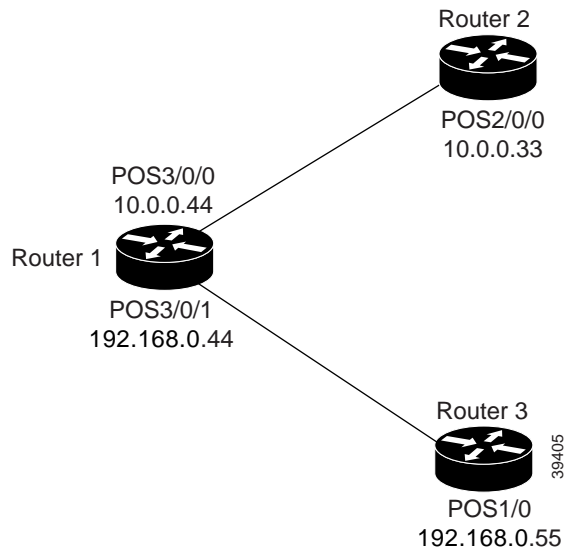
### Configuring Directly Connected MPLS LDP Sessions: Example

[Figure 1](#) shows a sample network for configuring directly connected LDP sessions.

This example configures the following:

- MPLS hop-by-hop forwarding for the POS links between Router 1 and Router 2 and between Router 1 and Router 3.
- LDP for label distribution between Router 1 and Router 2.
- TDP for label distribution between Router 1 and Router 3.
- A loopback interface and IP address for each LSR that can be used as the LDP router ID.



**Figure 1 Configuration of MPLS LDP****Note**

The configuration examples below show only the commands related to configuring LDP for Router 1, Router 2, and Router 3 in the sample network shown in [Figure 1](#).

**Router 1 Configuration**

```

ip cef distributed
interface Loopback0
ip address 172.16.0.11 255.255.255.255
!
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip
mpls label protocol ldp
!
interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip
mpls label protocol tdp

```

```

!Assumes R1 supports distributed CEF
!Loopback interface for LDP ID.

```

```

!Enable hop-by-hop MPLS forwarding
!Use LDP for this interface

```

```

!Enable hop-by-hop MPLS forwarding
!Use TDP for this interface

```

**Router 2 Configuration**

```

ip cef distributed
!
interface Loopback0
ip address 172.16.0.22 255.255.255.255
!
interface POS2/0/0
ip address 10.0.0.33 255.0.0.0
mpls ip
mpls label protocol ldp

```

```

!Assumes R2 supports distributed CEF
!Loopback interface for LDP ID.

```

```

!Enable hop-by-hop MPLS forwarding
!Use LDP for this interface

```

**Router 3 Configuration**

```

ip cef
!
interface Loopback0
ip address 172.16.0.33 255.255.255.255
!

```

```

!Assumes R3 does not support dCEF
!Loopback interface for LDP ID.

```

```

interface POS1/0
ip address 192.168.0.55 255.0.0.0
mpls ip                                !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp                !Use TDP for this interface

```

The LDP configuration for Router 1 uses the **mpls label protocol ldp** command in interface configuration mode, because some of its interfaces use LDP and some use TDP. Another way to configure Router 1 is to use the **mpls label protocol ldp** command in global configuration mode to configure LDP as the default protocol for interfaces and use the **mpls label protocol tdp** command in interface configuration mode to configure TDP for the POS3/0/1 link to Router 3. This alternative way to configure Router 1 is shown below:

#### Router 1 Configuration

```

ip cef distributed                      !Assumes R1 supports dCEF
mpls label protocol ldp                !Use LDP for the default protocol
!
interface Loopback0                    !Loopback interface for LDP ID.
ip address 172.16.0.11 255.255.255.255
interface POS3/0/0
ip address 10.0.0.44 255.0.0.0
mpls ip                                !Enable hop-by-hop MPLS forwarding
                                         !Use LDP (configured i/f default)

interface POS3/0/1
ip address 192.168.0.44 255.0.0.0
mpls ip                                !Enable hop-by-hop MPLS forwarding
mpls label protocol tdp                !Use TDP for this interface

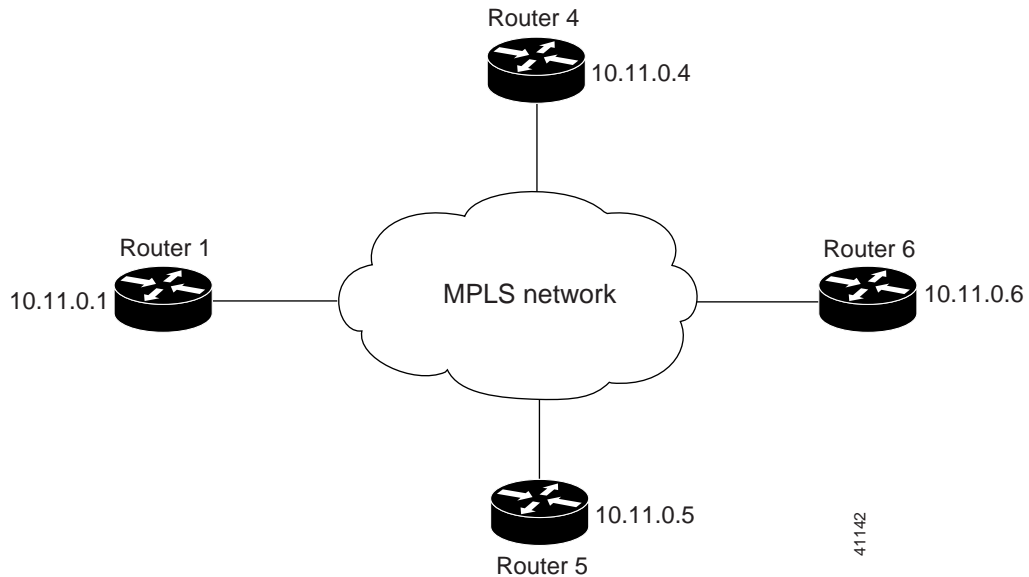
```

The configuration of Router 2 also uses the **mpls label protocol ldp** command in interface configuration mode. To specify LDP for all interfaces, use the **mpls label protocol ldp** command in global configuration mode without any interface **mpls label protocol** commands.

Configuring the **mpls ip** command on an interface triggers the transmission of discovery Hello messages for the interface.

## Establishing Nondirectly Connected MPLS LDP Sessions: Example

The following examples illustrate the configuration of platforms for MPLS LDP nondirectly connected sessions using the sample network shown in [Figure 2](#). Note that Routers 1, 4, 5, and 6 in this sample network are not directly connected to each other.

**Figure 2**      **Sample Network for Configuring LDP for Targeted Sessions**

The configuration example shows the following:

- Targeted sessions between Routers 1 and 4 use LDP. Routers 1 and 4 are both active.
- Targeted sessions between Routers 1 and 6 use LDP. Router 1 is active and Router 6 is passive.
- Targeted sessions between Routers 1 and 5 use TDP. Router 5 is active.

These examples assume that the active ends of the nondirectly connected sessions are associated with tunnel interfaces, such as MPLS traffic engineering tunnels. They show only the commands related to configuring LDP targeted sessions. The examples do not show configuration of the applications that initiate the targeted sessions.

### Router 1 Configuration

Tunnel interfaces Tunnel14 and Tunnel16 specify LDP for targeted sessions associated with these interfaces. The targeted session for Router 5 requires TDP. The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration from the Tunnel14 and Tunnel16.

```
ip cef distributed                !Router1 supports distributed CEF

mpls label protocol ldp          !Use LDP as default for all interfaces

interface Loopback0              !Loopback interface for LDP ID.
ip address 10.25.0.11 255.255.255.255

interface Tunnel14               !Tunnel to Router 4 requiring label distribution
tunnel destination 10.11.0.4    !Tunnel endpoint is Router 4
mpls ip                         !Enable hop-by-hop forwarding on the interface

interface Tunnel15               !Tunnel to Router 5 requiring label distribution
tunnel destination 10.11.0.5    !Tunnel endpoint is Router 5
mpls label protocol tdp         !Use TDP for session with Router 5
mpls ip                         !Enable hop-by-hop forwarding on the interface

interface Tunnel16               !Tunnel to Router 6 requiring label distribution
tunnel destination 10.11.0.6    !Tunnel endpoint is Router 6
```

```
mpls ip                                !Enable hop-by-hop forwarding on the interface
```

#### Router 4 Configuration

The **mpls label protocol ldp** command in global configuration mode makes it unnecessary to explicitly specify LDP as part of the configuration for the Tunnel41 targeted session with Router 1.

```
ip cef distributed                      !Router 4 supports distributed CEF

mpls label protocol ldp                !Use LDP as default for all interfaces

interface Loopback0                    !Loopback interface for LDP ID.
ip address 10.25.0.44 255.255.255.255

interface Tunnel41                      !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1           !Tunnel endpoint is Router 1
mpls ip                                !Enable hop-by-hop forwarding on the interface
```

#### Router 5 Configuration

Router 5 must use TDP for all targeted sessions. Therefore, its configuration includes the **mpls label protocol tdp** command.

```
ip cef                                !Router 5 supports CEF

mpls label protocol tdp                !Use TDP as default for all interfaces

interface Loopback0                    !Loopback interface for LDP ID.
ip address 10.25.0.55 255.255.255.255

interface Tunnel51                      !Tunnel to Router 1 requiring label distribution
tunnel destination 10.11.0.1           !Tunnel endpoint is Router 1
mpls ip                                !Enable hop-by-hop forwarding on the interface
```

#### Router 6 Configuration

By default, a router cannot be a passive neighbor in targeted sessions. Therefore, Router 1, Router 4, and Router 5 are active neighbors in any targeted sessions. The **mpls ldp discovery targeted-hello accept** command permits Router 6 to be a passive target in targeted sessions with Router 1. Router 6 can also be an active neighbor in targeted sessions, although the example does not include such a configuration.

```
ip cef distributed                      !Router 6 supports distributed CEF

interface Loopback0                    !Loopback interface for LDP ID.
ip address 10.25.0.66 255.255.255.255

mpls ldp discovery targeted-hellos accept from LDP_SOURCES
                                         !Respond to requests for targeted hellos
                                         !from sources permitted by acl LDP_SOURCES

ip access-list standard LDP_SOURCES      !Define acl for targeted hello sources.
permit 10.11.0.1                          !Accept targeted hello request from Router 1.
deny any                                  !Deny requests from other sources.
```

## Additional References

The following sections provide references related to MPLS LDP.

## Related Documents

Related Topic	Document Title
Configures LDP on every interface associated with a specified IGP instance.	<a href="#"><i>MPLS LDP Autoconfiguration</i></a>
Ensures that LDP is fully established before the IGP path is used for switching.	<a href="#"><i>MPLS LDP-IGP Synchronization</i></a>
Allows ACLs to control the label bindings that an LSR accepts from its peer LSRs.	<a href="#"><i>MPLS LDP Inbound Label Binding Filtering</i></a>
Enables standard, SNMP-based network management of the label switching features in Cisco IOS.	<a href="#"><i>MPLS Label Distribution Protocol MIB Version 8 Upgrade</i></a>

## Standards

Standard	Title
None	—

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB (draft-ietf-mpls-ldp-mib-08.txt)</li> <li>SNMP-VACM-MIB The View-based Access Control Model (ACM) MIB for SNMP</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 3036	<i>LDP Specification</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mo/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mo/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.:

- **mpls label protocol** (global configuration)
- **mpls ldp router-id**

# Feature Information for MPLS Label Distribution Protocol

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS Label Distribution Protocol Overview

Feature Name	Releases	Feature Information
MPLS Label Distribution Protocol	12.0(10)ST	This feature was introduced in Cisco IOS Release 12.0(10)ST, incorporating a new set of Multiprotocol Label Switching (MPLS) CLI commands implemented for use with Cisco routers and switches. The CLI commands in this release reflected MPLS command syntax and terminology, thus facilitating the orderly transition from a network using the Tag Distribution Protocol (TDP) to one using the Label Distribution Protocol (LDP).
	12.0(14)ST	
	12.1(2)T	
	12.1(8a)E	
	12.2(2)T	
	12.2(4)T	In Cisco IOS Release 12.0(14)ST, several new MPLS CLI commands were introduced, support for MPLS VPNs was added by means of a new <i>vrf vpn-name</i> parameter in certain existing commands, and other commands were modified to ensure consistent interpretation of associated <i>prefix-access-list</i> arguments by Cisco IOS software.
	12.2(8)T	
	12.0(21)ST	
	12.0(22)S	
	12.0(23)S	
	12.2(13)T	In Cisco IOS 12.1(2)T, this feature was integrated into this release. Also, the <b>debug mpls atm-ldp api</b> , <b>debug mpls atm-ldp routes</b> , and <b>debug mpls atm-ldp states</b> commands were modified.
	12.4(3)	
	12.4(5)	
		This feature was integrated into Cisco IOS Release 12.1(8a)E.
		This feature was integrated into Cisco IOS Release 12.2(2)T.

Table 2 Feature Information for MPLS Label Distribution Protocol Overview (continued)

Feature Name	Releases	Feature Information
		<p>In Cisco IOS Release 12.2(4)T, support was added for Cisco MGX 8850 and MGX 8950 switches equipped with a Cisco MGX RPM-PR card, and the VPI range in the <b>show mpls atm-ldp bindings</b> and <b>show mpls ip binding</b> commands was changed to 4095.</p> <p>In Cisco IOS Release 12.2(8)T, the <b>debug mpls atm-ldp failure</b> command was introduced.</p> <p>In Cisco IOS Release 12.0(21)ST, the <b>mpls ldp neighbor implicit-withdraw</b> command was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.0(22)S. The <b>mpls ldp neighbor targeted-session</b> command and the <b>interface</b> keyword for the <b>mpls ldp advertise-labels</b> command were added.</p> <p>This feature was integrated into Cisco IOS Release 12.0(23)S. Default values for the <b>mpls ldp discovery</b> command <b>holdtime</b> and <b>interval</b> keywords were changed.</p> <p>This feature was integrated into Cisco IOS Release 12.2(13)T.</p> <p>In Cisco IOS Release 12.4(3), the default MPLS label distribution protocol changed from TDP to LDP. See <a href="#">“LDP and TDP Support” section on page 2</a> for more information. If no protocol is explicitly configured by the <b>mpls label protocol</b> command, LDP is the default label distribution protocol. See the <b>mpls label protocol</b> (global configuration) command for more information.</p> <p>Also in Cisco IOS Release 12.4(3), LDP configuration commands are saved by using the MPLS form of the command rather than the tag-switching form. Previously, commands were saved by using the tag-switching form of the command, for backward compatibility. See the <a href="#">“Saving Configurations: MPLS/Tag Switching Commands” section on page 11</a> for more information.</p> <p>In Cisco IOS Release 12.4(5), the <b>vrf vrf-name</b> keyword/argument pair was added for the <b>mpls ldp router-id</b> command to allow you to associate the LDP router ID with a nondefault VRF.</p>

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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

© 1999-2008 Cisco Systems, Inc. All rights reserved.





# MPLS LDP Session Protection

---

**First Published: November 8, 2004**

**Last Updated: May 31, 2007**

The MPLS LDP Session Protection feature provides faster label distribution protocol convergence when a link recovers following an outage. MPLS LDP Session Protection protects a label distribution protocol (LDP) session between directly connected neighbors or an LDP session established for a traffic engineering (TE) tunnel.

## **Finding Feature Information in This Module**

*Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS LDP Session Protection](#)” section on page 23.*

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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

## Contents

- [Information About MPLS LDP Session Protection, page 2](#)
- [How to Configure MPLS LDP Session Protection, page 2](#)
- [Configuration Examples for MPLS LDP Session Protection, page 7](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for MPLS LDP Session Protection, page 23](#)



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

## Information About MPLS LDP Session Protection

MPLS LDP Session Protection maintains LDP bindings when a link fails. MPLS LDP sessions are protected through the use of LDP Hello messages. When you enable MPLS LDP, the label switched routers (LSRs) send messages to find other LSRs with which they can create LDP sessions.

- If the LSR is one hop from its neighbor, it is directly connected to its neighbor. The LSR sends out LDP Hello messages as User Datagram Protocol (UDP) packets to all the routers on the subnet. The hello message is called an LDP Link Hello. A neighboring LSR responds to the hello message and the two routers begin to establish an LDP session.
- If the LSR is more than one hop from its neighbor, it is not directly connected to its neighbor. The LSR sends out a directed hello message as a UDP packet, but as a unicast message specifically addressed to that LSR. The hello message is called an LDP Targeted Hello. The nondirectly connected LSR responds to the Hello message and the two routers establish an LDP session. (If the path between two LSRs has been traffic engineered and has LDP enabled, the LDP session between them is called a targeted session.)

MPLS LDP Session Protection uses LDP Targeted Hellos to protect LDP sessions. Take, for example, two directly connected routers that have LDP enabled and can reach each other through alternate IP routes in the network. An LDP session that exists between two routers is called an LDP Link Hello Adjacency. When MPLS LDP Session Protection is enabled, an LDP Targeted Hello Adjacency is also established for the LDP session. If the link between the two routers fails, the LDP Link Adjacency also fails. However, if the LDP peer is still reachable through IP, the LDP session stays up, because the LDP Targeted Hello Adjacency still exists between the routers. When the directly connected link recovers, the session does not need to be reestablished, and LDP bindings for prefixes do not need to be releared.

## How to Configure MPLS LDP Session Protection

This section explains how to configure and verify MPLS LDP Session Protection:

- [Enabling MPLS LDP Session Protection, page 2](#) (required)
- [Customizing MPLS LDP Session Protection, page 5](#) (optional)
- [Verifying MPLS LDP Session Protection, page 6](#) (optional)

### Enabling MPLS LDP Session Protection

You use the **mpls ldp session protection** command to enable MPLS LDP Session Protection. This command enables LDP sessions to be protected during a link failure. By default, the command protects all LDP sessions. The command has several options that enable you to specify which LDP sessions to protect. The **vrf** keyword lets you protect LDP sessions for a specified VRF. The **for** keyword lets you specify a standard IP access control list (ACL) of prefixes that should be protected. The **duration** keyword enables you to specify how long the router should retain the LDP Targeted Hello Adjacency following the loss of the LDP Link Hello Adjacency.

## Prerequisites

LSRs must be able to respond to LDP targeted hellos. Otherwise, the LSRs cannot establish a targeted adjacency. All routers that participate in MPLS LDP Session Protection must be enabled to respond to targeted hellos. Both neighbor routers must be configured for session protection or one router must be configured for session protection and the other router must be configured to respond to targeted hellos.

## Restrictions

This feature is not supported under the following circumstances:

- With TDP sessions
- With extended access lists
- With LC-ATM routers

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [distributed]
4. **interface loopback***number*
5. **ip address** {*prefix mask*}
6. **interface** *interface*
7. **mpls ip**
8. **mpls label protocol** {**ldp** | **tdp** | **both**}
9. **exit**
10. **mpls ldp session protection** [**vrf** *vpn-name*] [**for** *acl*] [**duration** *seconds*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef	Configures Cisco Express Forwarding.
Step 4	<b>interface loopbacknumber</b>  <b>Example:</b> Router(config)# interface Loopback0	Configures a loopback interface and enters interface configuration mode.
Step 5	<b>ip address {prefix mask}</b>  <b>Example:</b> Router(config-if)# ip address 10.25.0.11 255.255.255.255	Assigns an IP address to the loopback interface.
Step 6	<b>interface interface</b>  <b>Example:</b> Router(config-if)# interface POS3/0	Specifies the interface to configure.
Step 7	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding for a specified interface.
Step 8	<b>mpls label protocol {ldp   tdp   both}</b>  <b>Example:</b> Router(config-if)# mpls label protocol ldp	Configures the use of LDP on a specific interface or on all interfaces.  In interface configuration mode, the command sets the default label distribution protocol for the interface to be LDP, overriding any default set by the global <b>mpls label protocol</b> command.  In global configuration mode, the command sets all the interfaces to LDP.

	Command or Action	Purpose
Step 9	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits from interface configuration mode.
Step 10	<b>mpls ldp session protection</b> [ <b>vrf</b> <i>vpn-name</i> ] [ <b>for</b> <i>acl</i> ] [ <b>duration</b> <i>seconds</i> ]  <b>Example:</b> Router(config)# mpls ldp session protection	Enables MPLS LDP Session Protection.

## Customizing MPLS LDP Session Protection

You can modify MPLS LDP Session Protection by using the keywords in the **mpls ldp session protection** command. The following sections explain how to customize the feature.

### Specifying How Long an LDP Targeted Hello Adjacency Should Be Retained

The default behavior of the **mpls ldp session protection** command allows an LDP Targeted Hello Adjacency to exist indefinitely following the loss of an LDP Link Hello Adjacency. You can issue the **duration** keyword to specify the number of seconds (from 30 to 2,147,483) that the LDP Targeted Hello Adjacency is retained after the loss of the LDP Link Hello Adjacency. When the link is lost, a timer starts. If the timer expires, the LDP Targeted Hello Adjacency is removed.

### Specifying Which Routers Should Have MPLS LDP Session Protection

The default behavior of the **mpls ldp session protection** command allows MPLS LDP Session Protection for all neighbor sessions. You can issue either the **vrf** or **for** keyword to limit the number of neighbor sessions that are protected.

### Enabling MPLS LDP Session Protection on Specified VPN Routing and Forwarding Instances

If the router is configured with at least one VPN routing and forwarding (VRF) instance, you can use the **vrf** keyword to select which VRF is to be protected. You cannot specify more than one VRF with the **mpls ldp session protection** command. To specify multiple VRFs, issue the command multiple times.

### Enabling MPLS LDP Session Protection on Specified Peer Routers

You can create an access list that includes several peer routers. You can specify that access list with the **for** keyword to enable LDP Session Protection for the peer routers in the access control list.

## Verifying MPLS LDP Session Protection

To verify that LDP Session Protection has been correctly configured, perform the following steps.

### SUMMARY STEPS

1. show mpls ldp discovery
2. show mpls ldp neighbor
3. show mpls ldp neighbor detail

### DETAILED STEPS

#### Step 1 show mpls ldp discovery

Issue this command and check that the output contains xmit/recv to the peer router.

```
Router# show mpls ldp discovery
```

```
Local LDP Identifier:
 10.0.0.5:0
Discovery Sources:
Interfaces:
  ATM5/1/0.5 (ldp): xmit/recv
    LDP Id: 10.0.0.1:0
Targeted Hellos:
 10.0.0.5 -> 10.0.0.3 (ldp): active, xmit/recv
    LDP Id: 10.0.0.3:0
```

#### Step 2 show mpls ldp neighbor

Issue this command to check that the targeted hellos are active.

```
Router# show mpls ldp neighbor
```

```
Peer LDP Ident: 10.0.0.3:0; Local LDP Ident 10.0.0.5:0
TCP connection: 10.0.0.3.646 - 10.0.0.5.11005
State: Oper; Msgs sent/rcvd: 1453/1464; Downstream
Up time: 21:09:56
LDP discovery sources:
  Targeted Hello 10.0.0.5 -> 10.0.0.3, active
Addresses bound to peer LDP Ident:
 10.3.104.3      10.0.0.2      10.0.0.3
```

#### Step 3 show mpls ldp neighbor detail

Issue this command to check that the MPLS LDP Session Protection state is Ready or Protecting. If the second last line of the output shows Incomplete, the Targeted Hello Adjacency is not up yet.

```
Router# show mpls ldp neighbor detail
```

```
Peer LDP Ident: 10.16.16.16:0; Local LDP Ident 10.15.15.15:0
TCP connection: 10.16.16.16.11013 - 10.15.15.15.646
State: Oper; Msgs sent/rcvd: 53/51; Downstream; Last TIB rev sent 74
Up time: 00:11:32; UID: 1; Peer Id 0;
LDP discovery sources:
  Targeted Hello 10.15.15.15 -> 10.16.16.16, active, passive;
    holdtime: infinite, hello interval: 10000 ms
Addresses bound to peer LDP Ident:
 10.0.0.2      10.16.16.16      10.101.101.101 11.0.0.1
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Clients: Dir Adj Client
```

```
LDP Session Protection enabled, state: Protecting
duration: infinite
```

## Troubleshooting Tips

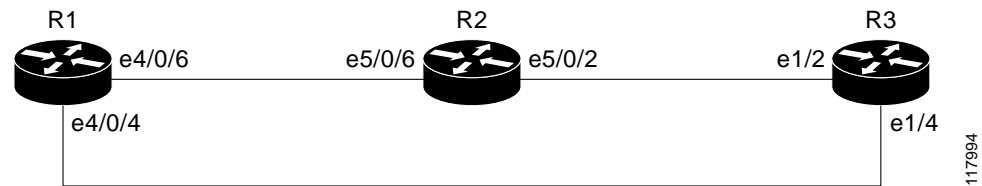
Use the **clear mpls ldp neighbor** command if you need to terminate an LDP session after a link goes down. This is useful for situations where the link needs to be taken out of service or needs to be connected to a different neighbor.

To enable the display of events related to MPLS LDP Session Protection, use the **debug mpls ldp session protection** command.

## Configuration Examples for MPLS LDP Session Protection

Figure 1 shows a sample configuration for MPLS LDP Session Protection.

**Figure 1** *MPLS LDP Session Protection Example*



### R1

```

redundancy
 no keepalive-enable
 mode hsa
!
ip cef distributed
no ip domain-lookup
multilink bundle-name both
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp router-id Loopback0 force
!
interface Loopback0
 ip address 10.0.0.1 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Multilink4
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 load-interval 30
 ppp multilink
 multilink-group 4
!
interface Ethernet1/0/0
 ip address 10.3.123.1 255.255.0.0

```

```

    no ip directed-broadcast
    !
interface Ethernet4/0/0
    no ip address
    no ip directed-broadcast
    shutdown
    !
interface Ethernet4/0/1
    description -- ip address 10.0.0.2 255.255.255.0
    no ip address
    no ip directed-broadcast
    shutdown
    !
interface Ethernet4/0/4
    ip address 10.0.0.1 255.0.0.0
    no ip directed-broadcast
    mpls label protocol ldp
    tag-switching ip
    !
interface Ethernet4/0/6
    ip address 10.0.0.1 255.0.0.0
    no ip directed-broadcast
    mpls label protocol ldp
    tag-switching ip
    !
interface Ethernet4/0/7
    ip address 10.0.0.1 255.0.0.0
    no ip directed-broadcast
    mpls label protocol ldp
    tag-switching ip
    !
router ospf 100
    log-adjacency-changes
    redistribute connected
    network 10.0.0.1 0.0.0.0 area 100
    network 10.0.0.0 0.255.255.255 area 100
    network 10.0.0.0 0.255.255.255 area 100
    network 10.0.0.0 0.255.255.255 area 100
    !
ip classless

```

## R2

```

redundancy
    no keepalive-enable
    mode hsa
    !
ip subnet-zero
ip cef distributed
mpls label protocol ldp
mpls ldp session protection
no mpls traffic-eng auto-bw timers frequency 0
tag-switching tdp router-id Loopback0 force
    !
interface Loopback0
    ip address 10.0.0.3 255.255.255.255
    no ip directed-broadcast
    !
interface Ethernet5/0/0
    no ip address
    no ip directed-broadcast
    shutdown
    full-duplex

```



```
!  
interface Ethernet5/0/2  
  ip address 10.0.0.1 255.0.0.0  
  no ip directed-broadcast  
  full-duplex  
  mpls label protocol ldp  
  tag-switching ip  
!  
interface Ethernet5/0/6  
  ip address 10.0.0.2 255.0.0.0  
  no ip directed-broadcast  
  ip load-sharing per-packet  
  full-duplex  
  mpls label protocol ldp  
  tag-switching ip  
!  
interface FastEthernet5/1/0  
  ip address 10.3.123.112 255.255.0.0  
  no ip directed-broadcast  
!  
router ospf 100  
  log-adjacency-changes  
  redistribute connected  
  network 10.0.0.3 0.0.0.0 area 100  
  network 10.0.0.0 0.255.255.255 area 100  
  network 10.0.0.0 0.255.255.255 area 100  
!  
ip classless
```

### R3

```
ip cef  
no ip domain-lookup  
mpls label range 200 100000 static 16 199  
mpls label protocol ldp  
no mpls traffic-eng auto-bw timers frequency 0  
tag-switching tdp router-id Loopback0 force  
!  
interface Loopback0  
  ip address 10.0.0.5 255.255.255.255  
  no ip directed-broadcast  
!  
interface Ethernet1/0  
  no ip address  
  no ip directed-broadcast  
  shutdown  
  half-duplex  
!  
interface Ethernet1/2  
  ip address 10.0.0.2 255.0.0.0  
  no ip directed-broadcast  
  full-duplex  
  mpls label protocol ldp  
  tag-switching ip  
!  
interface Ethernet1/4  
  ip address 10.0.0.2 255.0.0.0  
  no ip directed-broadcast  
  full-duplex  
  mpls label protocol ldp  
  tag-switching ip  
!  
router ospf 100  
  log-adjacency-changes
```

```
redistribute connected
network 10.0.0.5 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
!
ip classless
```

## Additional References

The following sections provide references related to the MPLS LDP Session Protection feature.

## Related Documents

Related Topic	Document Title
MPLS LDP	<a href="#">MPLS Label Distribution Protocol</a>
MPLS LDP-IGP synchronization	<a href="#">MPLS LDP-IGP Synchronization</a>
LDP autoconfiguration	<a href="#">LDP Autoconfiguration</a>

## Standards

Standards	Title
None	—

## MIBs

MIBs	MIBs Link
MPLS LDP MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 3036	<a href="#">LDP Specification</a>
RFC 3037	<a href="#">LDP Applicability</a>

## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this

module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp session protection**
- **mpls ldp session protection**
- **show mpls ldp neighbor**
- **Feature Information for MPLS LDP Session Protection**

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS LDP-IGP Synchronization

---

**First Published: November 20, 2004**

**Last Updated: September 2, 2009**

The MPLS LDP-IGP Synchronization feature ensures that the Label Distribution Protocol (LDP) is fully established before the Interior Gateway Protocol (IGP) path is used for switching.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature History for MPLS LDP-IGP Synchronization](#)” section on page 17.

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

## Contents

- [Prerequisites for MPLS LDP-IGP Synchronization, page 2](#)
- [Restrictions for MPLS LDP-IGP Synchronization, page 2](#)
- [Information About MPLS LDP-IGP Synchronization, page 2](#)
- [How to Configure MPLS LDP-IGP Synchronization, page 4](#)
- [Configuration Examples for MPLS LDP-IGP Synchronization, page 14](#)
- [Additional References, page 15](#)
- [Feature History for MPLS LDP-IGP Synchronization, page 17](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS LDP-IGP Synchronization

- This feature is supported only on interfaces that are running Open Shortest Path First (OSPF) or Intermediate System-to-System (IS-IS) processes.
- This feature works when LDP is enabled on interfaces with either the **mpls ip** command or the **mpls ldp autoconfig** command.

## Restrictions for MPLS LDP-IGP Synchronization

- In Cisco IOS Release 12.2(33)SB, and Cisco IOS Release 12.2(33)SRB, the MPLS LDP-IGP Synchronization feature is not supported with IS-IS. Only OSPF is supported.
- The Tag Distribution Protocol (TDP) is not supported. You must specify that the default label distribution protocol is LDP for a router or for an interface.
- This feature is not supported on tunnel interfaces or LC-ATM interfaces.
- This feature is not supported with interface-local label space or downstream-on-demand (DoD) requests.
- This feature does not support targeted LDP sessions. Therefore, Any Transport over MPLS (AToM) sessions are not supported.

## Information About MPLS LDP-IGP Synchronization

To configure the MPLS LDP-IGP Synchronization feature, you should understand the following concepts:

- [How MPLS LDP-IGP Synchronization Works, page 2](#)
- [MPLS LDP-IGP Synchronization with Peers, page 3](#)
- [MPLS LDP-IGP Synchronization Delay Timer, page 3](#)
- [MPLS LDP-IGP Synchronization Incompatibility with IGP Nonstop Forwarding, page 4](#)
- [MPLS LDP-IGP Synchronization Compatibility with LDP Graceful Restart, page 4](#)

## How MPLS LDP-IGP Synchronization Works

Packet loss can occur because the actions of the IGP and LDP are not synchronized. Packet loss can occur in the following situations:

- When an IGP adjacency is established, the router begins forwarding packets using the new adjacency before the LDP label exchange completes between the peers on that link.
- If an LDP session closes, the router continues to forward traffic using the link that is associated with the LDP peer rather than an alternate pathway with a fully synchronized LDP session.

The MPLS LDP-IGP Synchronization feature does the following:

- Provides a means to synchronize LDP and IGPs to minimize Multiprotocol Label Switching (MPLS) packet loss.
- Enables you to globally enable LDP-IGP synchronization on each interface that is associated with an IGP OSPF or IS-IS process.

- Provides a means to disable LDP-IGP synchronization on interfaces that you do not want enabled.
- Prevents MPLS packet loss due to synchronization conflicts.
- Works when LDP is enabled on interfaces using either the **mpls ip** or **mpls ldp autoconfig** command.

To enable LDP-IGP synchronization on each interface that belongs to an OSPF or IS-IS process, enter the **mpls ldp sync** command. If you do not want some of the interfaces to have LDP-IGP synchronization enabled, issue the **no mpls ldp igp sync** command on those interfaces.

If the LDP peer is reachable, the IGP waits indefinitely (by default) for synchronization to be achieved. To limit the length of time the IGP session must wait, enter the **mpls ldp igp sync holddown** command. If the LDP peer is not reachable, the IGP establishes the adjacency to enable the LDP session to be established.

When an IGP adjacency is established on a link but LDP-IGP synchronization is not yet achieved or is lost, the IGP advertises the max-metric on that link.

## MPLS LDP-IGP Synchronization with Peers

When the MPLS LDP-IGP Synchronization feature is enabled on an interface, LDP determines if any peer connected by the interface is reachable by looking up the peer's transport address in the routing table. If a routing entry (including longest match or default routing entry) for the peer exists, LDP assumes that LDP-IGP synchronization is required for the interface and notifies the IGP to wait for LDP convergence.

LDP-IGP synchronization with peers requires that the routing table be accurate for the peer's transport address. If the routing table shows there is a route for the peer's transport address, that route must be able to reach the peer's transport address. However, if the route is a summary route, a default route, or a statically configured route, it may not be the correct route for the peer. You must verify that the route in the routing table can reach the peer's transport address.

When the routing table has an inaccurate route for the peer's transport address, LDP cannot set up a session with the peer, which causes the IGP to wait for LDP convergence unnecessarily for the sync hold-down time.

## MPLS LDP-IGP Synchronization Delay Timer

Cisco IOS Release 12.0(32)SY and later releases of the MPLS LDP-IGP Synchronization feature provide the option to configure a delay time for MPLS LDP and IGP synchronization on an interface-by-interface basis. Normally, when LDP-IGP synchronization is configured, LDP notifies IGP as soon as LDP is converged. When the delay timer is configured, this notification is delayed. If you want to configure a delay time on an interface, use the **mpls ldp igp sync delay delay-time** command in interface configuration mode. To remove the delay timer from a specified interface, enter the **no mpls ldp igp sync delay** command. This command sets the delay time to 0 seconds, but leaves MPLS LDP-IGP synchronization enabled.

When LDP is fully established and synchronized, LDP checks the delay timer:

- If you configured a delay time, LDP starts the timer. When the timer expires, LDP checks that synchronization is still valid and notifies the OSPF process.
- If you did not configure a delay time, if synchronization is disabled or down, or if an interface was removed from an IGP process, LDP stops the timer and immediately notifies the OSPF process.

If you configure a new delay time while a timer is running, LDP saves the new delay time but does not reconfigure the running timer.

## MPLS LDP-IGP Synchronization Incompatibility with IGP Nonstop Forwarding

The MPLS LDP-IGP Synchronization feature is not supported during the startup period if IGP nonstop forwarding (NSF) is configured. The MPLS LDP-IGP Synchronization feature conflicts with IGP NSF when the IGP is performing NSF during startup. After the NSF startup is complete, the MPLS LDP-IGP Synchronization feature is supported.

## MPLS LDP-IGP Synchronization Compatibility with LDP Graceful Restart

LDP graceful restart protects traffic when an LDP session is lost. If an interface that supports a graceful-restart-enabled LDP session fails, MPLS LDP-IGP synchronization is still achieved on the interface while it is protected by Graceful Restart. MPLS LDP-IGP synchronization is eventually lost under the following circumstances

- If LDP fails to restart before the LDP Graceful Restart reconnect timer expires.
- If an LDP session restarts through other interfaces, but the LDP session on the protected interface fails to recover when the LDP Graceful Restart recovery timer expires.

## How to Configure MPLS LDP-IGP Synchronization

This section contains the following procedures:

- [Configuring MPLS LDP-IGP Synchronization with OSPF Interfaces, page 4](#) (required)
- [Disabling MPLS LDP-IGP Synchronization on Some OSPF Interfaces, page 6](#) (optional)
- [Verifying MPLS LDP-IGP Synchronization with OSPF, page 7](#) (optional)
- [Configuring MPLS LDP-IGP Synchronization with IS-IS Interfaces, page 8](#) (required)
- [Disabling MPLS LDP-IGP Synchronization on Some IS-IS Interfaces, page 12](#) (optional)
- [Verifying MPLS LDP-IGP Synchronization with IS-IS, page 12](#) (optional)

## Configuring MPLS LDP-IGP Synchronization with OSPF Interfaces

To configure MPLS LDP-IGP synchronization with OSPF interfaces, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol ldp**
5. **interface** *type number*
6. **ip address** *prefix mask*



7. **mpls ip**
8. **exit**
9. **router ospf process-id**
10. **network ip-address wildcard-mask area area-id**
11. **mpls ldp sync**
12. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Globally enables hop-by-hop forwarding.
Step 4	<b>mpls label protocol ldp</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.
Step 5	<b>interface type number</b>  <b>Example:</b> Router(config)# interface POS3/0	Specifies the interface to configure and enters interface configuration mode.
Step 6	<b>ip address prefix mask</b>  <b>Example:</b> Router(config-if)# ip address 10.25.0.11 255.255.255.255	Assigns an IP address to the interface.
Step 7	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Enables hop-by-hop forwarding on the interface.
Step 8	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode.

	Command or Action	Purpose
Step 9	<b>router</b> <i>ospf process-id</i>  <b>Example:</b> Router(config)# router ospf 1	Enables OSPF routing and enters router configuration mode.
Step 10	<b>network</b> <i>ip-address wildcard-mask area area-id</i>  <b>Example:</b> Router(config-router)# network 10.0.0.0 0.255.255.255 area 3	Defines an interface on which OSPF runs and defines the area ID for that interface.
Step 11	<b>mpls ldp sync</b>  <b>Example:</b> Router(config-router)# mpls ldp sync	Enables MPLS LDP-IGP synchronization for interfaces for an OSPF or an IS-IS process.
Step 12	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

## Disabling MPLS LDP-IGP Synchronization on Some OSPF Interfaces

When you issue the **mpls ldp sync** command, all of the interfaces that belong to an OSPF process are enabled for LDP-IGP synchronization. To remove LDP-IGP synchronization from some interfaces, use the **no** form of the **mpls ldp igp sync** command on those interfaces. The following configuration steps show how to disable LDP-IGP synchronization from some OSPF interfaces after they have been configured with LDP-IGP synchronization through the **mpls ldp sync** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp sync**
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface type number</b>  <b>Example:</b> Router(config)# interface POS3/0	Specifies the interface to configure and enters interface configuration mode.
Step 4	<b>no mpls ldp igp sync</b>  <b>Example:</b> Router(config-if)# no mpls ldp igp sync	Disables MPLS LDP-IGP synchronization for that interface.
Step 5	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Verifying MPLS LDP-IGP Synchronization with OSPF

After you configure the interfaces for LDP, OSPF, and LDP-IGP synchronization, verify that the configuration is working correctly using the **show mpls ldp igp sync** and **show ip ospf mpls ldp interface** commands.

## SUMMARY STEPS

1. **enable**
2. **show mpls ldp igp sync**
3. **show ip ospf mpls ldp interface**

## DETAILED STEPS

Step 1	<b>enable</b>  Enables privileged EXEC mode. Enter your password if prompted.
Step 2	<b>show mpls ldp igp sync</b>  The output of this command (as shown in the following example) shows that MPLS LDP-IGP synchronization is configured correctly, because LDP is configured and the SYNC status shows that synchronization is enabled.  Router# <b>show mpls ldp igp sync</b>

```
Ethernet0/0:
LDP configured; SYNC enabled.
SYNC status: sync achieved; peer reachable.
IGP holddown time: infinite.
Peer LDP Ident: 10.0.0.1:0
IGP enabled: OSPF 1
```

If MPLS LDP-IGP synchronization is not enabled on an interface, the output appears as follows:

```
Ethernet5/1:
LDP configured; LDP-IGP Synchronization not enabled.
```

### Step 3 **show ip ospf mpls ldp interface**

The output of the **show ip ospf mpls ldp interface** command in the following example shows that the interfaces are properly configured:

```
Router# show ip ospf mpls ldp interface

Ethernet3/0/0
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization: Yes
  Holddown timer is not configured
  Timer is not running
Ethernet3/0/2
  Process ID 1, Area 0
  LDP is configured through LDP autoconfig
  LDP-IGP Synchronization: Yes
  Holddown timer is not configured
  Timer is not running
```

## Configuring MPLS LDP-IGP Synchronization with IS-IS Interfaces



### Note

In Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB, the MPLS LDP-IGP Synchronization feature is not supported with IS-IS. Only OSPF is supported.

The following sections contain the steps and examples for configuring MPLS LDP-IGP synchronization for interfaces that are running IS-IS processes:

- [Configuring MPLS LDP-IGP Synchronization on All IS-IS Interfaces, page 8](#)
- [Configuring MPLS LDP-IGP Synchronization on an IS-IS Interface, page 10](#)

## Configuring MPLS LDP-IGP Synchronization on All IS-IS Interfaces

This section contains the steps for configuring the MPLS LDP-IGP Synchronization feature on all interfaces that are running IS-IS processes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**

4. **mpls label protocol ldp**
5. **router isis** *process-name*
6. **mpls ldp sync**
7. **mpls ldp autoconfig**
8. **exit**
9. **interface** *type number*
10. **ip address** *prefix mask*
11. **ip router isis** *process-name*
12. **mpls ip**
13. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Globally enables hop-by-hop forwarding.
Step 4	<b>mpls label protocol ldp</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.
Step 5	<b>router isis</b> <i>process-name</i>  <b>Example:</b> Router(config)# router isis ISIS	Enables the IS-IS protocol on the router, specifies an IS-IS process, and enters router configuration mode.
Step 6	<b>mpls ldp sync</b>  <b>Example:</b> Router(config-router)# mpls ldp sync	Enables MPLS LDP-IGP synchronization on interfaces belonging to an IS-IS process.
Step 7	<b>mpls ldp autoconfig</b>  <b>Example:</b> Router(config-router)# mpls ldp autoconfig	Configures auto-configuration to quickly configure the auto synchronization. When auto-configure is configured, auto-sync configuration is not required on any interfaces with MPLS enabled.

	Command or Action	Purpose
Step 8	<b>exit</b>  <b>Example:</b> Router(config-router)# exit	Exits router configuration mode and returns to global configuration mode.
Step 9	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface POS0/3	Specifies the interface to configure and enters interface configuration mode.
Step 10	<b>ip address</b> <i>prefix mask</i>  <b>Example:</b> Router(config-if)# ip address 10.25.25.11 255.255.255.0	Assigns an IP address to the interface.
Step 11	<b>ip router isis</b> <i>process-name</i>  <b>Example:</b> Router(config-if)# ip router isis ISIS	Enables IS-IS.
Step 12	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Enables MPLS IP.
Step 13	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Configuring MPLS LDP-IGP Synchronization on an IS-IS Interface

This section contains the steps for configuring the MPLS LDP-IGP Synchronization feature on an interface that is running an IS-IS process.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *prefix mask*
5. **mpls ldp igp sync**
6. **ip router isis**
7. **exit**
8. **router isis**
9. **mpls ldp sync**
10. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface type number</b>  <b>Example:</b> Router(config)# interface POS0/2	Specifies the interface to configure and enters interface configuration mode.
Step 4	<b>ip address prefix mask</b>  <b>Example:</b> Router(config-if)# ip address 10.50.72.4 255.0.0.0	Assigns an IP address to the interface.
Step 5	<b>mpls ldp igp sync</b>  <b>Example:</b> Router(config-if)# mpls ldp igp sync	Enables MPLS LDP-IGP synchronization.
Step 6	<b>ip router isis</b>  <b>Example:</b> Router(config-if)# ip router isis	Enables the IS-IS protocol for IP on the interface.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 8	<b>router isis</b>  <b>Example:</b> Router(config)# router isis	Enables IS-IS process on the router.
Step 9	<b>mpls ldp sync</b>  <b>Example:</b> Router(config-router)# mpls ldp sync	Enables LDP-IGP synchronization for interfaces that belongs to an IS-IS process.
Step 10	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

## Disabling MPLS LDP-IGP Synchronization on Some IS-IS Interfaces

When you issue the **mpls ldp sync** command, all of the interfaces that belong to an IS-IS process are enabled for LDP-IGP synchronization. To remove LDP-IGP synchronization from some interfaces, use the **no** form of the **mpls ldp igp sync** command on those interfaces. The following configuration steps show how to disable LDP-IGP synchronization from some IS-IS interfaces after they have been configured with LDP-IGP synchronization through the **mpls ldp sync** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp sync**
5. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface POS3/0	Specifies the interface to configure and enters interface configuration mode.
Step 4	<b>no mpls ldp igp sync</b>  <b>Example:</b> Router(config-if)# no mpls ldp igp sync	Disables MPLS LDP-IGP synchronization for that interface.
Step 5	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Verifying MPLS LDP-IGP Synchronization with IS-IS

After you configure the interfaces for LDP-IGP synchronization with IS-IS, you can verify that the configuration is working correctly with the **show isis mpls ldp** command.



## SUMMARY STEPS

1. **enable**
2. **show isis mpls ldp**

## DETAILED STEPS

---

**Step 1 enable**

Enables privileged EXEC mode. Enter your password if prompted.

**Step 2 show isis mpls ldp**

The output of the following command shows that IS-IS is configured on the interface (ISIS is UP) and that MPLS LDP-IGP synchronization with IS-IS is configured properly (SYNC achieved).

```
Router# show isis mpls ldp
```

```
Interface: POS0/2; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
  LDP enabled: NO
SYNC Information :
  Required: YES
  Achieved: YES
  IGP Delay: NO
  Holddown time: Infinite
  State: SYNC achieved
```

If MPLS LDP-IGP synchronization with IS-IS is not enabled on an interface, the output looks like the following:

```
Interface: Ethernet0; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
  LDP enabled: NO
SYNC Information :
  Required: NO
```

If MPLS LDP-IGP synchronization with IS-IS is configured but is not enabled, the output looks like the following:

```
Interface: Ethernet0/0; ISIS tag ISIS-1 enabled
ISIS is UP on interface
AUTOCONFIG Information :
  LDP enabled: YES
SYNC Information :
  Required: YES
  Achieved: NO
  IGP Delay: YES
  Holddown time: Infinite
  State: Holding down until SYNC
```

The IS-IS process holds down the adjacency of the interface until synchronization is enabled.

---

## Troubleshooting Tips

Use the **debug mpls ldp igp sync** command to display events related to MPLS LDP-IGP synchronization.

## Configuration Examples for MPLS LDP-IGP Synchronization

The following sections show examples for the MPLS LDP-IGP Synchronization feature with OSPF and IS-IS processes:

- [MPLS LDP-IGP Synchronization with OSPF: Example, page 14](#)
- [MPLS LDP-IGP Synchronization with IS-IS: Example, page 14](#)

### MPLS LDP-IGP Synchronization with OSPF: Example

The following configuration commands enable LDP for OSPF process 1. The **mpls ldp sync** command and the OSPF **network** commands enable LDP on interfaces POS0/0, POS0/1, and POS1/1, respectively. The **no mpls ldp igp sync** command on interface POS1/0 prevents LDP from being enabled on interface POS1/0, even though OSPF is enabled for that interface.

```
Router# configure terminal
Router(config)# interface POS0/0
Router(config-if)# ip address 10.0.0.1
Router(config-if)# mpls ip
!
Router(config)# interface POS0/1
Router(config-if)# ip address 10.0.1.1
Router(config-if)# mpls ip
!
Router(config)# interface POS1/1
Router(config-if)# ip address 10.1.1.1
Router(config-if)# mpls ip
!
Router(config)# interface POS1/0
Router(config-if)# ip address 10.1.0.1
Router(config-if)# mpls ip
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.0.255.255 area 3
Router(config-router)# network 10.1.0.0 0.0.255.255 area 3
Router(config-router)# mpls ldp sync
Router(config-router)# exit
Router(config)# interface POS1/0
Router(config-if)# no mpls ldp igp sync
```

### MPLS LDP-IGP Synchronization with IS-IS: Example



#### Note

In Cisco IOS Release 12.2(33)SRB and 12.2(33)SB, the MPLS LDP-IGP Synchronization feature is not supported with IS-IS. Only OSPF is supported.

The following commands configure MPLS LDP-IGP synchronization on interfaces POS0/2 and POS0/3, which are running IS-IS processes:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface POS0/2
Router(config-if)# ip router isis
Router(config-if)# exit
Router(config)# router isis
Router(config-router)# mpls ldp sync
!
!
Router(config)# interface POS0/3
Router(config-if)# ip router isis
Router(config-if)# exit
Router(config)# router isis
Router(config-router)# mpls ldp sync

```

## Additional References

The following sections provide references related to the MPLS LDP-IGP Synchronization feature.

### Related Documents

Related Topic	Document Title
MPLS LDP	<a href="#">MPLS Label Distribution Protocol</a>
MPLS LDP Autoconfiguration	<a href="#">MPLS LDP Autoconfiguration</a>
MPLS LDP Session Protection	<a href="#">MPLS LDP Session Protection</a>

### Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

### MIBs

MIBs	MIBs Link
MPLS LDP MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 3036	<a href="#"><i>LDP Specification</i></a>
RFC 3037	<a href="#"><i>LDP Applicability</i></a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature History for MPLS LDP-IGP Synchronization

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS LDP-IGP Synchronization

Feature Name	Releases	Feature Information
MPLS LDP-IGP Synchronization	12.0(30)S 12.0(32)SY 12.2(33)SB 12.2(33)SRB 15.0(1)M 12.3(14)T Cisco IOS XE Release 2.1	<p>The MPLS LDP-IGP Synchronization feature ensures that LDP is fully established before the IGP path is used for switching.</p> <p>In 12.0(30)S, this feature was introduced.</p> <p>In 12.0(32)SY, support for enabling synchronization on interfaces running Intermediate System-to-System (IS-IS) processes was added.</p> <p>In 12.2(33)SB, the feature was integrated. MPLS LDP-IGP synchronization for IS-IS is not supported in this release.</p> <p>In 12.2(33)SRB, the feature was integrated. MPLS LDP-IGP synchronization for IS-IS is not supported in this release.</p> <p>In 12.3(14)T, this feature was integrated. MPLS LDP-IGP synchronization for IS-IS is not supported in this release.</p> <p>In 15.0(1)M, support for enabling synchronization on interfaces running IS-IS processes was added.</p> <p>In XE 2.1, this feature was implemented on Cisco ASR 1000 Series Routers.</p> <p>The following commands were modified: <b>debug mpls ldp igp sync</b>, <b>mpls ldp igp sync</b>, <b>mpls ldp igp sync holddown</b>, <b>mpls ldp sync</b>, <b>show ip ospf mpls ldp interface</b>, <b>show isis mpls ldp</b>, and <b>show mpls ldp igp sync</b>.</p>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card,

and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# MPLS LDP Autoconfiguration

---

**First Published: November 8, 2004**

**Last Updated: November 25, 2009**

The MPLS LDP Autoconfiguration feature enables you to globally configure Label Distribution Protocol (LDP) on every interface associated with a specified Interior Gateway Protocol (IGP) instance.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS LDP Autoconfiguration](#)” section on page 13.

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

## Contents

- [Restrictions for MPLS LDP Autoconfiguration](#), page 2
- [Information About MPLS LDP Autoconfiguration](#), page 2
- [How to Configure MPLS LDP Autoconfiguration](#), page 2
- [Configuration Examples for MPLS LDP Autoconfiguration](#), page 10
- [Additional References](#), page 11
- [Feature Information for MPLS LDP Autoconfiguration](#), page 13



---

**Americas Headquarters:**

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

## Restrictions for MPLS LDP Autoconfiguration

The MPLS LDP Autoconfiguration feature has the following restrictions:

- In Cisco IOS Release 12.0(32)SY, the **mpls ldp autoconfig** command is supported only with the IS-IS interface. Other IGPs are not supported.
- If LDP is disabled globally, the **mpls ldp autoconfig** command fails and generates a console message explaining that LDP must first be enabled globally by means of the global **mpls ip** command.
- If the **mpls ldp autoconfig** command is configured for an IGP instance, you cannot issue the global **no mpls ip** command. To disable LDP, you must first issue the **no mpls ldp autoconfig** command.
- For interfaces running IS-IS processes, you can enable Multiprotocol Label Switching (MPLS) for each interface, using the router mode command **mpls ldp autoconfig** or **mpls ldp igp autoconfig** at the interface level.
- You specify that the default label distribution protocol is LDP for a router or for an interface. Tag Distribution Protocol (TDP) is not supported.
- The MPLS LDP Autoconfiguration feature is not supported on traffic engineering tunnel interfaces.

## Information About MPLS LDP Autoconfiguration

To enable LDP, you should configure it globally and on each interface where it is needed. Configuring LDP on many interfaces can be time-consuming. The following section provides information about autoconfiguration feature on OSPF and IS-IS interfaces:

- [MPLS LDP Autoconfiguration on OSPF and IS-IS Interfaces](#)

## MPLS LDP Autoconfiguration on OSPF and IS-IS Interfaces

The MPLS LDP Autoconfiguration feature enables you to globally enable LDP on every interface associated with an IGP instance. This feature is supported on OSPF and IS-IS IGPs. It provides a means to block LDP from being enabled on interfaces that you do not want enabled. The goal of the MPLS LDP Autoconfiguration feature is to make configuration easier, faster, and error free.

You issue the **mpls ldp autoconfig** command to enable LDP on each interface that is running an OSPF or IS-IS process. If you do not want some of the interfaces to have LDP enabled, you can issue the **no** form of the **mpls ldp igp autoconfig** command on those interfaces.

## How to Configure MPLS LDP Autoconfiguration

This section contains the following procedures:

- [Configuring MPLS LDP Autoconfiguration with OSPF Interfaces, page 3](#) (required)
- [Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces, page 4](#) (optional)
- [Verifying MPLS LDP Autoconfiguration with OSPF, page 5](#) (optional)
- [Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces, page 6](#) (required)
- [Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces, page 8](#) (optional)



- [Verifying MPLS LDP Autoconfiguration with IS-IS, page 9](#) (optional)

## Configuring MPLS LDP Autoconfiguration with OSPF Interfaces

The following steps explain how to configure LDP for interfaces running OSPF processes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **mpls label protocol ldp**
5. **interface** *type number*
6. **ip address** *prefix mask*
7. **exit**
8. **router ospf** *process-id*
9. **network** *ip-address wildcard-mask area area-id*
10. **mpls ldp autoconfig** [**area** *area-id*]
11. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Globally enables hop-by-hop forwarding.
Step 4	<b>mpls label protocol ldp</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.
Step 5	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface POS 3/0	Specifies the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
Step 6	<b>ip address</b> <i>prefix mask</i>  <b>Example:</b> Router(config-if)# ip address 10.0.0.11 255.255.255.255	Assigns an IP address to the interface.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode.
Step 8	<b>router ospf</b> <i>process-id</i>  <b>Example:</b> Router(config)# router ospf 1	Enables OSPF routing and enters router configuration mode.
Step 9	<b>network</b> <i>ip-address wildcard-mask area area-id</i>  <b>Example:</b> Router(config-router)# network 10.0.0.0 0.0.255.255 area 3	Specifies the interface on which OSPF runs and defines the area ID for that interface.
Step 10	<b>mpls ldp autoconfig</b> [ <i>area area-id</i> ]  <b>Example:</b> Router(config-router)# mpls ldp autoconfig area 3	Enables the MPLS LDP Autoconfiguration feature to enable LDP on interfaces belonging to an OSPF process. <ul style="list-style-type: none"> <li>If no area is specified, the command applies to all interfaces associated with the OSPF process. If an area ID is specified, then only interfaces associated with that OSPF area are enabled with LDP.</li> </ul>
Step 11	<b>end</b>  <b>Example:</b> Router(config-router)# end	Exits router configuration mode and returns to privileged EXEC mode.

## Disabling MPLS LDP Autoconfiguration from Selected OSPF Interfaces

When you issue the **mpls ldp autoconfig** command, all the interfaces that belong to an OSPF area are enabled for LDP. To remove LDP from some interfaces, use the **no mpls ldp igp autoconfig** command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with the MPLS LDP Autoconfiguration feature with the **mpls ldp autoconfig** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp autoconfig**
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface POS 3/0	Specifies the interface to configure and enters interface configuration mode.
Step 4	<b>no mpls ldp igp autoconfig</b>  <b>Example:</b> Router(config-if)# no mpls ldp igp autoconfig	Disables LDP for that interface.
Step 5	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Verifying MPLS LDP Autoconfiguration with OSPF

The following steps explain how to verify the MPLS LDP Autoconfiguration feature.

## SUMMARY STEPS

1. **enable**
2. **show mpls interfaces** [*type number* / **vrf** *vpn-name*] [**all**] [**detail**] [**internal**]
3. **show mpls ldp discovery** [**vrf** *vpn-name* / **all**] [**detail**]

## DETAILED STEPS

- |               |   |
|---------------|---|
| <b>Step 1</b> | <b>enable</b><br><br>Enables privileged EXEC mode. Enter your password if prompted.   |
| <b>Step 2</b> | <b>show mpls interfaces</b> [ <i>type number</i> / <b>vrf</b> <i>vpn-name</i> ] [ <b>all</b> ] [ <b>detail</b> ] [ <b>internal</b> ]<br><br>The <b>show mpls interfaces</b> command displays the method used to enable LDP on an interface: <ul style="list-style-type: none"> <li>• If LDP is enabled by the <b>mpls ldp autoconfig</b> command, the output displays:               <pre>IP labeling enabled (ldp):   IGP config</pre> </li> </ul> |

- If LDP is enabled by the **mpls ip** command, the output displays:

```
IP labeling enabled (ldp):
  Interface config
```

- If LDP is enabled by the **mpls ip** command and the **mpls ldp autoconfig** command, the output displays:

```
IP labeling enabled (ldp):
  Interface config
  IGP config
```

The following example shows that LDP was enabled on the interface by both the **mpls ip** and **mpls ldp autoconfig** commands:

```
Router# show mpls interfaces Serial 2/0 detail
```

```
Interface Serial2/0:
  IP labeling enabled (ldp):
    Interface config
    IGP config
  LSP Tunnel labeling enabled
  BGP labeling not enabled
  MPLS operational
  Fast Switching Vectors:
    IP to MPLS Fast Switching Vector
    MPLS Turbo Vector
    MTU = 1500
```

### Step 3 **show mpls ldp discovery [vrf vpn-name / all] [detail]**

The **show mpls ldp discovery detail** command also shows how LDP was enabled on the interface. In the following example, LDP was enabled by both the **mpls ip** and **mpls ldp autoconfig** commands:

```
Router# show mpls ldp discovery detail
```

```
Local LDP Identifier:
  10.11.11.11:0
Discovery Sources:
Interfaces:
  Serial2/0 (ldp): xmit/rcv
    Enabled: Interface config, IGP config;
    Hello interval: 5000 ms; Transport IP addr: 10.11.11.11
    LDP Id: 10.10.10.10:0
    Src IP addr: 10.0.0.1; Transport IP addr: 10.10.10.10
    Hold time: 15 sec; Proposed local/peer: 15/15 sec
```

## Configuring MPLS LDP Autoconfiguration with IS-IS Interfaces

The following steps explain how to configure the MPLS LDP Autoconfiguration feature for interfaces that are running IS-IS processes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip address prefix mask**

5. **ip router isis**
6. **exit**
7. **mpls ip**
8. **mpls label protocol ldp**
9. **router isis**
10. **mpls ldp autoconfig** [*level-1* / *level-2*]
11. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface POS 0/2	Specifies the interface to configure and enters interface configuration mode.
Step 4	<b>ip address</b> <i>prefix mask</i>  <b>Example:</b> Router(config-if)# ip address 10.50.72.4 255.0.0.0	Assigns an IP address to the interface.
Step 5	<b>ip router isis</b>  <b>Example:</b> Router(config-if)# ip router isis	Enables IS-IS for IP on the interface.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	Exits interface configuration mode.
Step 7	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Globally enables hop-by-hop forwarding.
Step 8	<b>mpls label protocol ldp</b>  <b>Example:</b> Router(config)# mpls label protocol ldp	Specifies LDP as the default label distribution protocol.

	Command or Action	Purpose
Step 9	<code>router isis</code>  <b>Example:</b> <code>Router(config)# router isis</code>	Enables an IS-IS process on the router and enters router configuration mode.
Step 10	<code>mpls ldp autoconfig [level-1   level-2]</code>  <b>Example:</b> <code>Router(config-router)# mpls ldp autoconfig</code>	Enables the LDP for interfaces that belong to an IS-IS process.
Step 11	<code>end</code>  <b>Example:</b> <code>Router(config-router)# end</code>	Exits router configuration mode and returns to privileged EXEC mode.

## Disabling MPLS LDP Autoconfiguration from Selected IS-IS Interfaces

When you issue the **mpls ldp autoconfig** command, all the interfaces that belong to an IS-IS process are enabled for LDP. To remove LDP from some interfaces, use the **no mpls ldp igp autoconfig** command on those interfaces. The following configuration steps show how to disable LDP from some of the interfaces after they were configured with the MPLS LDP Autoconfiguration feature with the **mpls ldp autoconfig** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no mpls ldp igp autoconfig**
5. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> <code>Router(config)# interface POS 3/0</code>	Specifies the interface to configure and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<code>no mpls ldp igp autoconfig</code>  <b>Example:</b> Router(config-if)# no mpls ldp igp autoconfig	Disables LDP for that interface.
Step 5	<code>end</code>  <b>Example:</b> Router(config-if)# end	Exits interface configuration mode and returns to privileged EXEC mode.

## Verifying MPLS LDP Autoconfiguration with IS-IS

You can verify that the MPLS LDP Autoconfiguration feature is working correctly with the **show isis mpls ldp** command.

### SUMMARY STEPS

1. **enable**
2. **show isis mpls ldp**

### DETAILED STEPS

#### Step 1 **enable**

Enables privileged EXEC mode.

#### Step 2 **show isis mpls ldp**

The output of the following **show isis mpls ldp** command shows that IS-IS is configured on the interface and that LDP is enabled:

```
Router# show isis mpls ldp
```

```
Interface: POS0/2; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
  LDP enabled: YES
  SYNC Information :
    Required: NO
```

The output shows :

- IS-IS is up.
- LDP is enabled.

If the MPLS LDP Autoconfiguration feature is not enabled on an interface, the output looks like the following:

```
Interface: Ethernet0; ISIS tag null enabled
ISIS is UP on interface
AUTOCONFIG Information :
  LDP enabled: NO
  SYNC Information :
    Required: NO
```

## Troubleshooting Tips

You can use the **debug mpls ldp autoconfig** command to display events that are related to the MPLS LDP Autoconfiguration feature.

## Configuration Examples for MPLS LDP Autoconfiguration

The following sections show examples for the MPLS LDP Autoconfiguration feature with OSPF and IS-IS processes.

- [MPLS LDP Autoconfiguration with OSPF: Example, page 10](#)
- [MPLS LDP Autoconfiguration with IS-IS: Examples, page 10](#)

### MPLS LDP Autoconfiguration with OSPF: Example

The following configuration commands enable LDP for OSPF process 1 area 3. The **mpls ldp autoconfig area 3** command and the OSPF **network** commands enable LDP on POS interfaces 0/0, 0/1, and 1/1. The **no mpls ldp igp autoconfig** command on POS interface 1/0 prevents LDP from being enabled on POS interface 1/0, even though OSPF is enabled for that interface.

```
configure terminal
interface POS 0/0
 ip address 10.0.0.1 255.0.0.0
!
interface POS 0/1
 ip address 10.0.1.1 255.0.0.1
!
interface POS 1/1
 ip address 10.1.1.1 255.255.0.0
!
interface POS 1/0
 ip address 10.1.0.1 0.1.0.255
 exit
!
router ospf 1
 network 10.0.0.0 0.0.255.255 area 3
 network 10.1.0.0 0.0.255.255 area 3
 mpls ldp autoconfig area 3
 end
interface POS 1/0
 no mpls ldp igp autoconfig
```

### MPLS LDP Autoconfiguration with IS-IS: Examples

The following example shows the configuration of the MPLS LDP Autoconfiguration feature on POS0/2 and 0/3 interfaces, which are running IS-IS processes:

```
configure terminal
interface POS 0/2
 ip address 10.0.0.1 255.0.0.1
 ip router isis
!
interface POS 0/3
 ip address 10.1.1.1 255.0.1.0
 ip router isis
```



```

exit

mpls ip
mpls label protocol ldp
router isis
mpls ldp autoconfig

```

## Additional References

The following sections provide references related to the MPLS LDP Autoconfiguration feature.

## Related Documents

Related Topic	Document Title
MPLS commands	<a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>
MPLS LDP	<a href="#">MPLS Label Distribution Protocol</a>
The MPLS LDP-IGP Synchronization feature	<a href="#">MPLS LDP-IGP Synchronization</a>
The MPLS LDP Session Protection feature	<a href="#">MPLS LDP Session Protection</a>
Configuring integrated IS-IS	<a href="#">Integrated IS-IS Routing Protocol Overview</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature	—

## MIBs

MIB	MIBs Link
MPLS LDP MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3036	<a href="#">LDP Specification</a>
RFC 3037	<a href="#">LDP Applicability</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for MPLS LDP Autoconfiguration

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS LDP Autoconfiguration

Feature Name	Releases	Feature Information
MPLS LDP Autoconfiguration	12.0(30)S 12.0(32)SY 12.2(28)SB 12.2(33)SRB 12.3(14)T 15.0(1)M 12.2(33)XNE	<p>This feature enables you to globally configure LDP on every interface associated with a specified Interior Gateway Protocol (IGP) instance.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About MPLS LDP Autoconfiguration, page 2</a></li> <li>• <a href="#">How to Configure MPLS LDP Autoconfiguration, page 2</a></li> </ul> <p>In Cisco IOS Release 12.0(30)S, this feature was introduced with support for OSPF.</p> <p>In Cisco IOS Release 12.0(32)SY, support for IS-IS was added.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB with support for OSPF.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>This feature was integrated into Cisco IOS Release 12.3(14)T with support for OSPF.</p> <p>In Release 15.0(1)M, support for IS-IS was added.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)XNE with support for IS-IS on the Cisco 10000 series router.</p> <p>The following commands were modified: <b>mpls ldp autoconfig</b>, <b>mpls ldp igp autoconfig</b>, <b>show isis mpls ldp</b>, and <b>show mpls ldp discovery</b>.</p>

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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# MPLS—LDP MD5 Global Configuration

---

**First Published: February 28, 2006**

**Last Updated: July 11, 2008**

The MPLS—LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages.

This document provides information about and configuration information for the global configuration of LDP MD5 protection.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS—LDP MD5 Global Configuration”](#) section on [page 20](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS—LDP MD5 Global Configuration, page 2](#)
- [Restrictions for MPLS—LDP MD5 Global Configuration, page 2](#)
- [Information About MPLS—LDP MD5 Global Configuration, page 2](#)
- [How to Configure the MPLS—LDP MD5 Global Configuration Feature, page 5](#)
- [Configuration Examples for Configuring the MPLS—LDP MD5 Global Configuration Feature, page 16](#)



---

**Americas Headquarters:**

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

© 2006—2008 Cisco Systems, Inc. All rights reserved.

- [Additional References, page 18](#)
- [Command Reference, page 19](#)
- [Glossary, page 22](#)
- [Feature Information for MPLS—LDP MD5 Global Configuration, page 20](#)

## Prerequisites for MPLS—LDP MD5 Global Configuration

- Cisco Express Forwarding or distributed Cisco Express Forwarding must be enabled on the label switch router (LSR).
- Routing (static or dynamic) must be configured for the LSR.
- Multiprotocol Label Switching (MPLS) LDP must be configured on the LSR. However, you can configure LDP MD5 protection before you configure MPLS LDP. You can then use LDP MD5 protection after you configure MPLS LDP.
- A Virtual Private Network (VPN) routing and forwarding instance (VRF) must be configured if you want to configure MPLS LDP MD5 global configuration for a VRF. If you delete a VRF, the LDP MD5 global configuration for that VRF is automatically removed.

## Restrictions for MPLS—LDP MD5 Global Configuration

MD5 protection described in this document applies only to the LDP sessions. All enhancements described in this document do not affect Tag Distribution Protocol (TDP) sessions.

## Information About MPLS—LDP MD5 Global Configuration

Before you configure the MPLS—LDP MD5 Global Configuration feature, you must understand the following:

- [Enhancements to LDP MD5 Protection for LDP Messages Between Peers, page 2](#)
- [LDP MD5 Password Configuration Information, page 3](#)
- [LDP MD5 Password Configuration for Routing Tables, page 4](#)

## Enhancements to LDP MD5 Protection for LDP Messages Between Peers

The MPLS—LDP MD5 Global Configuration feature provides the following enhancements to the LDP support of MD5 passwords:

- You can specify peers for which MD5 protection is required. This can prevent the establishment of LDP sessions with unexpected peers.
- You can configure passwords for groups of peers. This increases the scalability of LDP password configuration management.
- The established LDP session with a peer is not automatically torn down when the password for that peer is changed. The new password is used the next time an LDP session is established with the peer.

- You can control when the new password is used. You can configure the new password on the peer before forcing the use of the new password.
- If the neighboring nodes support graceful restart, then LDP sessions are gracefully restarted. The LDP MD5 password configuration is checkpointed to the standby Route Processors (RPs). The LDP MD5 password is used by the router when the new active RP attempts to establish LDP sessions with neighbors after the switchover.

LDP session, advertisement, and notification messages are exchanged between two LDP peers over a TCP connection. You can configure the TCP MD5 option to protect LDP messages that are exchanged over a TCP connection. You can configure this protection for each potential LDP peer. As a result, an LDP ignores any LDP hello messages sent from an LSR for which you have not configured a password. (LDP tries to establish an LDP session with each neighbor from which a hello message is received.)

Before the introduction of the MPLS—LDP MD5 Global Configuration feature, you needed to configure a separate password for each LDP peer for which you wanted MD5 protection. This was the case even when the same password was used for multiple LDP peers. Before this feature, LDP would tear down LDP sessions with a peer immediately if a password for that peer had changed.

## LDP MD5 Password Configuration Information

Before the introduction of the MPLS—LDP MD5 Global Configuration feature, the command used for configuring a password for an LDP neighbor was **mpls ldp neighbor [vrf vrf-name] ip-address password [0 | 7] password**. This command configures a password for one neighbor whose router ID is the IP address in the specified VRF. An LSR can have zero or one such configuration for each LDP neighbor.

You can use the commands provided by the MPLS—LDP MD5 Global Configuration feature to configure passwords for LDP neighbors.

You must understand how LDP determines the password for an LDP session between peers before you configure MD5 password protection for your network. LDP determines the passwords for its sessions based on the commands that you enter.

You can enter an **mpls ldp password vrf vrf-name required [for acl]** command, either with an optional *acl* argument that permits the LDP router ID of the neighbor or without an *acl* argument. Make sure that you enter a command that configures a password. Otherwise, LDP might not establish a session with the neighbor in question.

For the commands in the following password-determining process, *A.B.C.D:N* represents the LDP neighbor in VRF *vpn1* and the neighbor LDP ID:

- *A.B.C.D* is the neighbor router ID.
- *N* is the neighbor label space ID.

To determine the password for an LDP session for the neighbor label space *A.B.C.D:N*, LDP looks at the password commands in the order indicated by the following statements:

- If you configured this command:

**mpls ldp neighbor vrf vpn1 A.B.C.D password pwd-nbr**

The LDP session password is *pwd-nbr*. LDP looks no further and uses the password you specify.

- Otherwise, LDP looks to see if you configured one or more **mpls ldp vrf vpn1 password option** commands. LDP considers the commands in order of the ascending *number* arguments (*number-1st* to *number-n*). For example:

**mpls ldp vrf vpn1 password option number-1st for acl-1st pwd-1st**

LDP compares the peer router ID of the neighbor (*A.B.C.D*) with this command. If *A.B.C.D* is permitted by the command access list *acl-1st*, the session password is the command password, that is, *pwd-1st*.

If *A.B.C.D* is not permitted by *acl-1st*, LDP looks at the command with the next ascending *number* argument (*number-2nd*):

**mpls ldp vrf vpn1 password option *number-2nd* for *acl-2nd* *pwd-2nd***

If *A.B.C.D* is permitted by the command access list *acl-2nd*, the session password is *pwd-2nd*.

If *A.B.C.D* is not permitted by the access list *acl-2nd*, LDP continues checking *A.B.C.D* against access lists until LDP:

- Finds *A.B.C.D* permitted by an access list. Then the command password is the session password.
- Has processed the *number-nth* argument of this command (*n* being the highest *number* argument you configured for this command).
- If the **mpls ldp vrf vpn1 password option *number-nth* for *acl-nth* *pwd-nth*** command produces no match and, therefore no password, LDP looks to see if you configured the following command:

**mpls ldp password vrf vpn1 fallback *pwd-fback***

If you configured this command, the session password is *pwd-fback*.

- Otherwise, if LDP has not found a password, you did not configure a password for the session. LDP does not use MD5 protection for the session TCP connection.

## LDP MD5 Password Configuration for Routing Tables

The MPLS—LDP MD5 Global Configuration feature introduces commands that can establish password protection for LDP sessions between LDP neighbors or peers. These commands can apply to routes in the global routing table or in a VRF.

By default, if the **vrf** keyword is not specified in the command, the command applies to the global routing table. The following sample commands would apply to routes in the global routing table:

```
Router# mpls ldp password required
Router# mpls ldp password option 15 for 99 pwd-acl
Router# mpls ldp password fallback pwd-fbck
```

You can configure LDP MD5 password protection for routes in a VRF only when the VRF is configured on the LSR. If you specify a VRF name and a VRF with that name is not configured on the LSR, LDP prints out a warning and discards the command. If you remove a VRF, LDP deletes the password configuration for that VRF. The following sample commands would apply to routes in a VRF, for example, VRF vpn1:

```
Router# mpls ldp vrf vpn1 password required
Router# mpls ldp vrf vpn1 password option 15 for 99 pwd-acl
Router# mpls ldp vrf vpn1 password fallback pwd-flbk
```



# How to Configure the MPLS—LDP MD5 Global Configuration Feature

Perform the following tasks to configure the MPLS—LDP MD5 Global Configuration feature:

- [Identifying LDP Neighbors for LDP MD5 Password Protection, page 5](#) (required)
- [Configuring an LDP MD5 Password for LDP Sessions, page 7](#) (required)
- [Verifying the LDP MD5 Configuration, page 14](#) (optional)

## Password Requirements for LDP Sessions

You might require password protection for a certain set of neighbors for security reasons (for example, to prevent LDP sessions being established with unauthorized peers, or to block spoofed TCP messages). To enforce this security, you can configure a password requirement for LDP sessions with those neighbors that must have MD5 protection (TCP session uses a password).

If you configure a password requirement for a neighbor and you did not configure a password for the neighbor, LDP tears down the LDP sessions with the neighbor. LDP also tears down the LDP sessions with the neighbor if you configured a password requirement and a password and the password is not used in the LDP sessions.

If a password is required for a neighbor and the LDP sessions with the neighbor are established to use a password, any configuration that removes the password for the neighbor causes the LDP sessions to be torn down.

To avoid unnecessary LDP session flapping, you should perform the task as described in this section and use caution when you change LDP passwords.

## Identifying LDP Neighbors for LDP MD5 Password Protection

Perform the following task to identify LDP neighbors for LDP MD5 password protection.

### Prerequisites

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide MD5 protection. For example:

- You might have several customers that all use the same core routers. To ensure security you might want to provide each customer with a different password.
- You could have defined several departmental VRFs in your network. You could provide password protection for each VRF.
- Certain groups of peers might require password protection for security reasons. Password protection prevents unwanted LDP sessions.

Before you start to configure passwords for LDP sessions, you must identify neighbors or groups of peers for which you want to provide LDP MD5 password protection. This task uses the network in [Figure 1](#) to show how you might identify LDP neighbors for LDP MD5 protection.

After you identify LDP neighbors or a group of peers for LDP MD5 protection, you must decide if password protection is mandatory and what password commands to use for each peer.

## SUMMARY STEPS

1. Identify LDP neighbors or groups of peers for LDP MD5 password protection.
2. Decide what LDP MD5 protection is required for each neighbor or group of peers.

## DETAILED STEPS

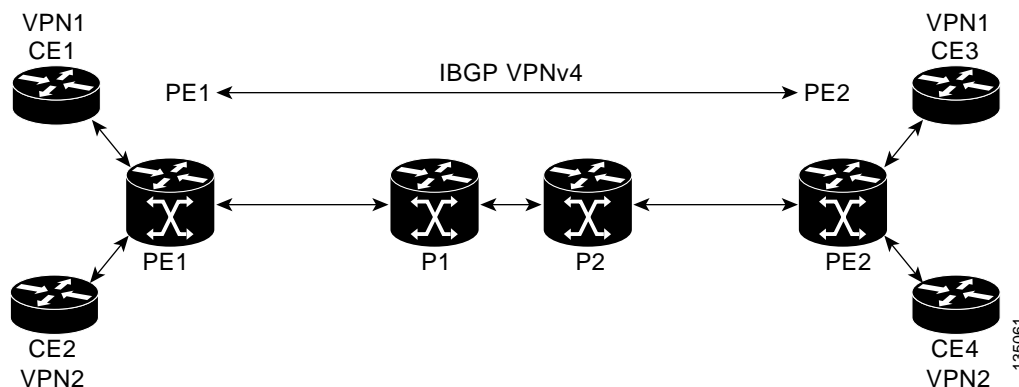
**Step 1** Identify LDP neighbors or groups of peers for LDP MD5 password protection.

This task uses the network in [Figure 1](#) to show how you might identify LDP neighbors for LDP MD5 protection.

[Figure 1](#) shows a sample network that has the following topology:

- Carrier Supporting Carrier (CSC) is configured between provider edge (PE) router PE1 and customer edge (CE) router CE1 and between PE1 and CE2.
- Internal Border Gateway Protocol (IBGP) Virtual Private Network (VPN) IPv4 (VPNv4) to support Layer 3 VPNs is configured between PE1 and PE2.
- CE1 and CE3 are in VRF VPN1. CE2 and CE4 are in a different VRF, VPN2.

**Figure 1** Sample Network: Identifying LDP Neighbors for LDP MD5 Protection



For the sample network in [Figure 1](#), you could configure separate passwords on PE1 for the following:

- VRF VPN1
- VRF VPN2

You could also configure a password requirement on PE1 for P1, P2, CE1 and CE2.

**Step 2** Decide what LDP MD5 protection is required for each neighbor or group of peers.

- If you need to set up a password for an LDP session with one peer or neighbor, for example, from PE1 to CE1, you could use the `mpls ldp neighbor [vrf vrf-name] ip-address password [0 | 7] password-string` command, where `ip-address` is the router ID of the neighbor. See the [“Configuring an LDP MD5 Password for LDP Sessions”](#) section on page 7 for instructions.
- If you need to set up an LDP session password for a set of peers, for example for P1 and P2, you could set up an access list that permits access to these routers and denies access to all others. See the [“Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers”](#) section on page 12 for instructions.

- If you want to require a password for communication among VRF vpn1 members, you can configure a password requirement and password for VRF vpn1. If your network contains several VRFs, you can configure a password for each VRF. See the [“Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF”](#) section on page 10 for instructions.

## Configuring an LDP MD5 Password for LDP Sessions

This section contains information about and instructions for configuring an LDP MD5 password for LDP sessions. You configure an LDP MD5 password to protect your routers from unwanted LDP sessions and provide LDP session security. You can provide LDP session security for a specific neighbor, or for LDP peers from a specific VRF or from the global routing table, or for a specific set of LDP neighbors.

After you have identified the LDP neighbor, LDP neighbors, or LDP peers in your network for which you want LDP MD5 password protection, perform the following procedures, as you require, to configure an LDP MD5 password for LDP sessions:

- [Configuring an LDP MD5 Password for a Specified Neighbor, page 7](#)
- [Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF, page 10](#)
- [Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers, page 12](#)

## Configuring an LDP MD5 Password for a Specified Neighbor

Perform the following task to configure an LDP MD5 password for a specified neighbor.

LDP looks first for a password between the router and neighbor that is configured with the **mpls ldp neighbor [vrf vrf-name] ip-address password pwd-string** command. If a password is configured with this command, LDP uses that password before checking passwords configured by other commands.

You must add a configuration command for each neighbor or peer for which you want password protection.

### Prerequisites

Identify the LDP neighbor or peer for which you want MD5 password protection.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp neighbor [vrf vrf-name] ip-address password [0 | 7] password-string**
4. **end**
5. **show mpls ldp neighbor [vrf vrf-name | all] [ip-address | interface] [detail] [graceful-restart]**
6. **show mpls ldp neighbor [vrf vrf-name] [ip-address | interface] password [pending | current]**
7. **show mpls ldp discovery [vrf vrf-name | all] [detail]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ldp neighbor</b> [ <i>vrf vrf-name</i> ] <i>ip-address</i> <b>password</b> [ <i>0</i>   <i>7</i> ] <i>password-string</i>  <b>Example:</b> Router(config)# mpls ldp neighbor vrf vpn1 10.1.1.1 password nbrcelpwd	Configures a password key for computing MD5 checksums for the session TCP connection with the specified neighbor. <ul style="list-style-type: none"> <li>The <b>vrf</b> <i>vrf-name</i> keyword-argument pair specifies the VPN routing and forwarding instance for the specified neighbor.</li> <li>The <i>ip-address</i> argument specifies the router ID (IP address) that identifies a neighbor.</li> <li>The [<b>0</b>   <b>7</b>] keywords specify whether the password that follows is encrypted: <ul style="list-style-type: none"> <li><b>0</b> specifies a clear-text (nonencrypted) password.</li> <li><b>7</b> specifies a Cisco proprietary encrypted password.</li> </ul> </li> <li>The <i>password-string</i> argument defines the password key to be used for computing MD5 checksums for the session TCP connection with the specified neighbor.</li> </ul>
Step 4	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	<p><code>show mpls ldp neighbor [vrf vrf-name   all]</code>  <code>[ip-address   interface] [detail]</code>  <code>[graceful-restart]</code></p> <p><b>Example:</b>  Router# show mpls ldp neighbor vrf vpn1 detail</p>	<p>Displays the status of LDP sessions.</p> <ul style="list-style-type: none"> <li>• The <b>vrf vrf-name</b> keyword-argument pair displays the LDP neighbors for the specified VRF instance (<i>vrf-name</i>).</li> <li>• The <b>all</b> keyword displays LDP neighbor information for all VPNs, including those in the default routing domain.</li> <li>• The <i>ip-address</i> argument identifies the neighbor with the IP address for which you configured password protection.</li> <li>• The <i>interface</i> argument defines the LDP neighbors accessible over this interface.</li> <li>• The <b>detail</b> keyword displays information in long form, including password information for this neighbor. Here are the items displayed: <ul style="list-style-type: none"> <li>– An indication as to whether a password is mandatory for this neighbor (required or not required)</li> <li>– The password source (neighbor, fallback or number [option number])</li> <li>– An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale)</li> </ul> </li> <li>• The <b>graceful-restart</b> keyword displays per-neighbor graceful restart information.</li> </ul>

	Command or Action	Purpose
Step 6	<p><code>show mpls ldp neighbor [vrf vrf-name] [ip-address   interface] password [pending   current]</code></p> <p><b>Example:</b> Router# show mpls ldp neighbor vrf vpn1 password</p>	<p>Displays password information used in established LDP sessions.</p> <ul style="list-style-type: none"> <li>The <b>vrf vrf-name</b> keyword-argument pair displays the LDP neighbors for the specified VRF instance (<i>vrf-name</i>).</li> <li>The <b>ip-address</b> argument identifies the neighbor with the IP address for which you configured password protection.</li> <li>The <b>interface</b> argument defines the LDP neighbors accessible over this interface.</li> <li>The <b>pending</b> keyword displays LDP sessions whose passwords are different from that in the current configuration.</li> <li>The <b>current</b> keyword displays LDP sessions whose password is the same as that in current configuration.</li> </ul> <p>If you do not specify an optional keyword for this command, password information for all established LDP sessions is displayed.</p>
Step 7	<p><code>show mpls ldp discovery [vrf vrf-name   all] [detail]</code></p> <p><b>Example:</b> Router# show mpls ldp discovery vrf vpn1 detail</p>	<p>Displays the status of the LDP discovery process.</p> <ul style="list-style-type: none"> <li>The <b>vrf vrf-name</b> keyword-argument pair displays the neighbor discovery information for the specified VRF instance (<i>vrf-name</i>).</li> <li>The <b>all</b> keyword displays LDP discovery information for all VPNs, including those in the default routing domain.</li> <li>The <b>detail</b> keyword displays detailed information about all LDP discovery sources on an LSR.</li> </ul>

## Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF

Perform the following task to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. You can also use this task to configure an LDP MD5 password for LDP sessions with peers from the global routing table.

This task provides you with LDP session protection with peers from a particular VRF or the global routing table. If you want a password requirement, you can use the **mpls ldp password required** command.

If only LDP sessions with a set of LDP neighbors need MD5 protection, configure a standard IP access list that10 permits the desired set of LDP neighbors and denies the rest. See the [“Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers”](#) section on page 12.

### Prerequisites

Identify LDP peers for which you want MD5 password protection.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp [vrf vrf-name] password fallback [0 | 7] password**
4. **mpls ldp [vrf vrf-name] password required [for acl]**
5. **end**
6. **show mpls ldp discovery [vrf vrf-name | all] [detail]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ldp [vrf vrf-name] password fallback [0   7] password</b>  <b>Example:</b> Router(config)# mpls ldp vrf vpn1 password fallback 0 vrfpwdvppn1	Configures an MD5 password for LDP sessions with peers. <ul style="list-style-type: none"> <li>• The <b>vrf vrf-name</b> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>• The <b>[0   7]</b> keywords specify whether the password that follows is encrypted: <ul style="list-style-type: none"> <li>– <b>0</b> specifies a clear-text (nonencrypted) password.</li> <li>– <b>7</b> specifies a Cisco proprietary encrypted password.</li> </ul> </li> <li>• The <i>password</i> argument specifies the MD5 password to be used for the LDP sessions with peers whose connections are established through a named VRF or the global routing table.</li> </ul> <p>The example sets up an MD5 password for a VRF.</p>
Step 4	<b>mpls ldp [vrf vrf-name] password required [for acl]</b>  <b>Example:</b> Router(config)# mpls ldp vrf vpn1 password required	Specifies that LDP must use a password when establishing a session between LDP peers. <ul style="list-style-type: none"> <li>• The <b>vrf vrf-name</b> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>• The <b>for acl</b> keyword-argument pair names an access list that specifies that a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the <i>acl</i> argument.</li> </ul>

	Command or Action	Purpose
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.
Step 6	<b>show mpls ldp discovery</b> [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ] [ <b>detail</b> ]  <b>Example:</b> Router# show mpls ldp discovery detail	Displays the status of the LDP discovery process. <ul style="list-style-type: none"> <li>The <b>vrf</b> <i>vrf-name</i> keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (<i>vrf-name</i>).</li> <li>The <b>all</b> keyword displays LDP discovery information for all VPNs, including those in the default routing domain.</li> <li>The <b>detail</b> keyword displays detailed information about all LDP discovery sources on an LSR.</li> </ul> Use this command to verify that password configuration is correct for all LDP neighbors.

## Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers

Perform the following task to configure an LDP MD5 password for LDP sessions with a selected group of peers.

If only LDP sessions with a selected group of peers need MD5 protection, configure a standard IP access list that permits sessions with the desired group of peers (identified by LDP router IDs) and denies session with the rest. Configuring a password and password requirement for these neighbors or peers provides security by preventing LDP sessions from being established with unauthorized peers.

### Prerequisites

Identify the groups of peers for which you want MD5 password protection and define an access list that permits LDP sessions with the group of peers you require.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp** [**vrf** *vrf-name*] **password option** *number* **for** *acl* [**0** | **7**] *password*
4. **mpls ldp** [**vrf** *vrf-name*] **password required** [**for** *acl*]
5. **end**
6. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**] [**detail**]



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls ldp [vrf vrf-name] password option number for acl [0   7] password</b>  <b>Example:</b> Router(config)# mpls ldp password option 25 for 10 aclpwdfor10	Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list. <ul style="list-style-type: none"> <li>The <b>vrf vrf-name</b> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>The <i>number</i> argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The valid range is 1–32767.</li> <li>The <b>for acl</b> keyword-argument pair specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access list values (1–99) can be used for the <i>acl</i> argument.</li> <li>The <b>[0   7]</b> keywords specifies whether the password that follows is encrypted: <ul style="list-style-type: none"> <li><b>0</b> specifies a clear-text (nonencrypted) password.</li> <li><b>7</b> specifies a Cisco proprietary encrypted password.</li> </ul> </li> <li>The <i>password</i> argument specifies the MD5 password to be used for the specified LDP sessions.</li> </ul>
Step 4	<b>mpls ldp [vrf vrf-name] password required [for acl]</b>  <b>Example:</b> Router(config)# mpls ldp password required for 10	Specifies that LDP must use a password when establishing a session between LDP peers. <ul style="list-style-type: none"> <li>The <b>vrf vrf-name</b> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>The <b>for acl</b> keyword-argument pair names an access list. The access list specifies a password is mandatory only for LDP sessions with neighbors whose LDP router IDs are permitted by the list. Only standard IP access lists can be used for the <i>acl</i> argument.</li> </ul>

	Command or Action	Purpose
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.
Step 6	<b>show mpls ldp discovery [vrf vrf-name   all] [detail]</b>  <b>Example:</b> Router# show mpls ldp discovery detail	<p>Displays the status of the LDP discovery process.</p> <ul style="list-style-type: none"> <li>The <b>vrf vrf-name</b> keyword-argument pair displays the neighbor discovery information for the specified VPN routing and forwarding instance (<i>vrf-name</i>).</li> <li>The <b>all</b> keyword displays LDP discovery information for all VPNs, including those in the default routing domain.</li> <li>The <b>detail</b> keyword displays detailed information about all LDP discovery sources on an LSR.</li> </ul> <p>Use this command to verify password configuration is correct for all LDP neighbors.</p>

## Verifying the LDP MD5 Configuration

Perform the following task to verify that the LDP MD5 secure sessions are as you configured for all LDP neighbors.

### SUMMARY STEPS

1. **enable**
2. **show mpls ldp discovery detail**
3. **show mpls ldp neighbor detail**
4. **show mpls ldp neighbor password [pending | current]**
5. **exit**

### DETAILED STEPS

#### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

#### Step 2 **show mpls ldp discovery detail**

Use this command to verify that the LDP MD5 password information is as you configured for each neighbor. For example:

```
Router# show mpls ldp discovery detail

Local LDP Identifier:
 10.1.1.1:0
Discovery Sources:
Interfaces:
```

```

Ethernet1/0 (ldp): xmit/recv
  Hello interval: 5000 ms; Transport IP addr: 10.1.1.1
  LDP Id: 10.4.4.4:0
  Src IP addr: 10.0.20.4; Transport IP addr: 10.4.4.4
  Hold time: 15 sec; Proposed local/peer: 15/15 sec
  Password: not required, none, stale
Targeted Hellos:
  10.1.1.1 -> 10.3.3.3 (ldp): passive, xmit/recv
    Hello interval: 10000 ms; Transport IP addr: 10.1.1.1
    LDP Id: 10.3.3.3:0
    Src IP addr: 10.3.3.3; Transport IP addr: 10.3.3.3
    Hold time: 90 sec; Proposed local/peer: 90/90 sec
    Password: required, neighbor, in use

```

The Password field might display any of the following for the status of the password:

- Required or not required—Indicates whether password configuration is required.
- Neighbor, none, option #, or fallback—Indicates the password source when the password was configured.
- In use (current) or stale (previous)—Indicates the current LDP session password usage status.

Look at the output of the command to verify your configuration.

### Step 3 show mpls ldp neighbor detail

Use this command to verify that the password information for a neighbor is as you configured. For example:

Router# **show mpls ldp neighbor detail**

```

Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
  TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
  Password: required, neighbor, in use
  State: Oper; Msgs sent/rcvd: 167/167; Downstream; Last TIB rev sent 9
  Up time: 02:24:02; UID: 5; Peer Id 3;
  LDP discovery sources:
    Targeted Hello 10.1.1.1 -> 10.3.3.3, passive;
      holdtime: 90000 ms, hello interval: 10000 ms
  Addresses bound to peer LDP Ident:
    10.3.3.3      10.0.30.3
  Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
  TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
  Password: not required, none, stale
  State: Oper; Msgs sent/rcvd: 9/9; Downstream; Last TIB rev sent 9
  Up time: 00:05:35; UID: 6; Peer Id 1;
  LDP discovery sources:
    Ethernet1/0; Src IP addr: 10.0.20.4
      holdtime: 15000 ms, hello interval: 5000 ms
  Addresses bound to peer LDP Ident:
    10.0.40.4      10.4.4.4      10.0.20.4
  Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab

```

### Step 4 show mpls ldp neighbor password [pending | current]

Use this command to verify that LDP sessions are using the password configuration that you expect, either the same as or different from that in the current configuration. The **pending** keyword displays information for LDP sessions whose password is different from that in the current configuration. The **current** keyword displays information for LDP sessions whose password is the same as that in the current configuration.

For example:

```
Router# show mpls ldp neighbor password
```

```
Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
Password: not required, none, stale
State: Oper; Msgs sent/rcvd: 57/57
Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
Password: required, neighbor, in use
State: Oper; Msgs sent/rcvd: 216/215
```

```
Router# show mpls ldp neighbor password pending
```

```
Peer LDP Ident: 10.4.4.4:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.4.4.4.11017 - 10.1.1.1.646
Password: not required, none, stale
State: Oper; Msgs sent/rcvd: 57/57
```

```
Router# show mpls ldp neighbor password current
```

```
Peer LDP Ident: 10.3.3.3:0; Local LDP Ident 10.1.1.1:0
TCP connection: 10.3.3.3.11018 - 10.1.1.1.646
Password: required, neighbor, in use
State: Oper; Msgs sent/rcvd: 216/215
```

This command displays password information used in established LDP sessions. If you do not enter an optional **pending** or **current** keyword for the command, password information for all established LDP sessions is displayed.

#### Step 5 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Configuration Examples for Configuring the MPLS—LDP MD5 Global Configuration Feature

This section contains the following example for configuring the MPLS—LDP MD5 Global Configuration feature:

- [Configuring an LDP MD5 Password for LDP Sessions: Examples, page 16](#)

## Configuring an LDP MD5 Password for LDP Sessions: Examples

The section contains the following examples for configuring an LDP MD5 password for LDP sessions:

- [Configuring an LDP MD5 Password for LDP Sessions for a Specified Neighbor: Example, page 17](#)
- [Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF: Example, page 17](#)

- [Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers: Example, page 17](#)

## Configuring an LDP MD5 Password for LDP Sessions for a Specified Neighbor: Example

The following example shows how to configure an LDP MD5 password for LDP sessions for a specified neighbor:

```
enable
configure terminal
mpls ldp vrf vpn1 10.1.1.1 password nbrscrtpwd
end
```

This sets up nbrscrtpwd as the password to use for LDP sessions for the neighbor whose LDP router ID is 10.1.1.1. Communication with this neighbor is through VRF vpn1.

## Configuring an LDP MD5 Password for LDP Sessions with Peers from a Specified VRF: Example

The following example shows how to configure an LDP MD5 password for LDP sessions with peers from a specified VRF. The password vrfpwdvpn1 is configured for use with LDP peers that communicate using VRF vpn1. A password is required; otherwise, LDP tears down the session.

```
enable
configure terminal
mpls ldp vrf vpn1 password fallback vrfpwdvpn1
mpls ldp vrf vpn1 password required
end
```

The following example shows how to configure a password that is used for sessions for peers that communicate using the global routing table:

```
enable
configure terminal
mpls ldp password fallback vrfpwdvppn1
end
```

## Configuring an LDP MD5 Password for LDP Sessions with a Selected Group of Peers: Example

The following example shows how to configure an LDP MD5 password for LDP sessions with a selected group of peers. The required password aclpwdfor10 is configured for access list 10. Only those LDP router IDs permitted in access list 10 are required to use the password.

```
enable
configure terminal
mpls ldp password option 25 for 10 aclpwdfor10
mpls ldp password required for 10
end
```

Access list 10 might look something like this:

```
enable
configure terminal
access-list 10 permit 10.1.1.1
access-list 10 permit 10.3.3.3
access-list 10 permit 10.4.4.4
access-list 10 permit 10.1.1.1
access-list 10 permit 10.2.2.2
end
```

# Additional References

The following sections provide references related to the MPLS—LDP MD5 Global Configuration feature.

## Related Documents

Related Topic	Document Title
Configuration tasks for LDP	<a href="#">MPLS LDP MD5 Global Configuration</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **mpls ldp password fallback**
- **mpls ldp password option**
- **mpls ldp password required**
- **show mpls ldp discovery**
- **show mpls ldp neighbor**
- **show mpls ldp neighbor password**

## Feature Information for MPLS—LDP MD5 Global Configuration

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---



**Table 1**      **Feature Information for MPLS—LDP MD5 Global Configuration**

Feature Name	Releases	Feature Information
MPLS—LDP MD5 Global Configuration	12.2(28)SB 12.0(32)SY 12.2(33)SRB 12.4(20)T	<p>The MPLS—LDP MD5 Global Configuration feature provides enhancements to the Label Distribution Protocol (LDP) implementation of the Message Digest 5 (MD5) password. This feature allows you to enable LDP MD5 globally instead of on a per-peer basis. Using this feature you can set up password requirements for a set of LDP neighbors to help prevent unauthorized peers from establishing LDP sessions and to block spoofed TCP messages.</p> <p>In 12.2(28)SB, this feature was introduced.</p> <p>In 12.0(32)SY, this feature was integrated into Cisco IOS Release 12.0(32)SY.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Enhancements to LDP MD5 Protection for LDP Messages Between Peers, page 2</a></li> <li>• <a href="#">LDP MD5 Password Configuration Information, page 3</a></li> <li>• <a href="#">LDP MD5 Password Configuration for Routing Tables, page 4</a></li> <li>• <a href="#">Password Requirements for LDP Sessions, page 5</a></li> <li>• <a href="#">Identifying LDP Neighbors for LDP MD5 Password Protection, page 5</a></li> <li>• <a href="#">Identifying LDP Neighbors for LDP MD5 Password Protection, page 5</a></li> <li>• <a href="#">Configuring an LDP MD5 Password for LDP Sessions, page 7</a></li> <li>• <a href="#">Verifying the LDP MD5 Configuration, page 14</a></li> </ul> <p>The following commands were modified by this feature:  <b>mpls ldp password fallback, mpls ldp password option, mpls ldp password required, show mpls ldp discovery, show mpls ldp neighbor, show mpls ldp neighbor password.</b></p>

# Glossary

**BGP**—Border Gateway Protocol. An interdomain routing protocol that replaces External Gateway Protocol (EGP). BGP systems exchange reachability information with other BGP systems. BGP is defined by RFC 1163.

**EGP**—Exterior Gateway Protocol. An internet protocol for exchanging routing information between autonomous systems. EGP is documented in RFC 904. EGP is not to be confused with the general term exterior gateway protocol. EGP is an obsolete protocol that was replaced by Border Gateway Protocol (BGP).

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

**CSC**—Carrier Supporting Carrier. A situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

**LDP**—Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers that is used in the negotiation of the labels used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LDP peer**—A label switch router (LSR) that is the receiver of label space information from another LSR. If an LSR has a label space to advertise to another LSR, or to multiple LSRs, one Label Distribution Protocol (LDP) session exists for each LSR (LDP peer) receiving the label space information.

**MD5**—Message Digest 5. A one-way hashing algorithm that produces a 128-bit hash. Both MD5 and Secure Hash Algorithm (SHA) are variations on MD4 and are designed to strengthen the security of the MD4 hashing algorithm. Cisco uses hashes for authentication within the IPSec framework. SNMP v.2 uses MD5 for message authentication, to verify the integrity of the communication, to authenticate the message origin, and to check its timeliness.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic through use of labels. Each label instructs the routers and the switches in the network where to forward a packet based on preestablished IP routing information.

**PE router**—provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) processing occurs in the PE router.

**VPN**—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic forwarded from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

**VRF**—A VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0807R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.





# MPLS LDP—Lossless MD5 Session Authentication

---

**First Published: November 30, 2007**

**Last Updated: July 11, 2008**

The MPLS LDP—Lossless MD5 Session Authentication feature enables a Label Distribution Protocol (LDP) session to be password-protected without tearing down and reestablishing the LDP session.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS LDP—Lossless MD5 Session Authentication” section on page 31](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS LDP—Lossless MD5 Session Authentication, page 2](#)
- [Restrictions for MPLS LDP—Lossless MD5 Session Authentication, page 2](#)
- [Information About MPLS LDP—Lossless MD5 Session Authentication, page 2](#)
- [How to Configure MPLS LDP—Lossless MD5 Session Authentication, page 6](#)
- [Configuration Examples for MPLS LDP—Lossless MD5 Session Authentication, page 16](#)
- [Additional References, page 29](#)
- [Command Reference, page 30](#)
- [Feature Information for MPLS LDP—Lossless MD5 Session Authentication, page 31](#)



---

**Americas Headquarters:**

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

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

# Prerequisites for MPLS LDP—Lossless MD5 Session Authentication

The MPLS LDP—Lossless MD5 Session Authentication feature is an enhancement to the MPLS LDP MD5 Global Configuration feature. Before configuring the MPLS LDP—Lossless MD5 Session Authentication feature, refer to the [MPLS—LDP MD5 Global Configuration](#) feature module for more information on how the message digest algorithm 5 (MD5) works with MPLS LDP to ensure that LDP segments remain properly protected.

**Note**

The MPLS LDP—Lossless MD5 Session Authentication feature must be configured before MPLS LDP is configured.

Configure the following features on the label switch router (LSR) before configuring the MPLS LDP—Lossless MD5 Session Authentication feature:

- Cisco Express Forwarding or distributed Cisco Express Forwarding
- Static or dynamic routing
- MPLS Virtual Private Network (VPN) routing and forwarding (VRFs) instances for MPLS VPNs
- MPLS LDP—Lossless MD5 Session Authentication for the MPLS VPN VRFs

**Note**

If a VRF is deleted, then the lossless MD5 session authentication for that VRF is automatically removed.

## Restrictions for MPLS LDP—Lossless MD5 Session Authentication

MD5 protection applies to LDP sessions between peers. Tag Distribution Protocol (TDP) sessions between peers are not protected.

## Information About MPLS LDP—Lossless MD5 Session Authentication

You should understand the following concepts before configuring the MPLS LDP—Lossless MD5 Session Authentication feature:

- [How MPLS LDP Messages in MPLS LDP—Lossless MD5 Session Authentication are Exchanged, page 3](#)
- [The Evolution of MPLS LDP MD5 Password Features, page 3](#)
- [Keychains Use with MPLS LDP—Lossless MD5 Session Authentication, page 4](#)
- [Application of Rules to Overlapping Passwords, page 4](#)
- [Password Rollover Period Guidelines, page 5](#)
- [Resolving LDP Password Problems, page 5](#)

## How MPLS LDP Messages in MPLS LDP—Lossless MD5 Session Authentication are Exchanged

MPLS LDP messages (discovery, session, advertisement, and notification messages) are exchanged between LDP peers through two channels:

- LDP discovery messages are transmitted as User Datagram Protocol (UDP) packets to the well-known LDP port.
- Session, advertisement, and notification messages are exchanged through a TCP connection established between two LDP peers.

The MPLS LDP—Lossless MD5 Session Authentication feature allows an LDP session to be password-protected without tearing down and reestablishing the LDP session. The MD5 password can be implemented and changed without interrupting the LDP session.

## The Evolution of MPLS LDP MD5 Password Features

The initial version of LDP MD5 protection allowed authentication to be enabled between two LDP peers and each segment sent on the TCP connection was verified between the peers. Authentication was configured on both LDP peers using the same password; otherwise, the peer session was not established. The **mpls ldp neighbor** command was issued with the **password** keyword. When MD5 protection was enabled, the router tore down the existing LDP sessions and established new sessions with the neighbor router.

An improved MD5 protection feature, called MPLS—LDP MD5 Global Configuration, was later introduced that allowed LDP MD5 to be enabled globally instead of on a per-peer basis. Using this feature, password requirements for a set of LDP neighbors could be configured. The MPLS LDP MD5 Global Configuration feature also improved the ability to maintain the LDP session. The LDP session with a peer was not automatically torn down when the password for that peer was changed. The new password was implemented the next time an LDP session was established with the peer.

The MPLS LDP—Lossless MD5 Session Authentication feature is based on the MPLS LDP MD5 Global Configuration feature. However, the MPLS LDP—Lossless MD5 Session Authentication feature provides the following enhancements:

- Activate or change LDP MD5 session authentication without interrupting the LDP session.
- Configure multiple passwords, so one password can be used now and other passwords later.
- Configure asymmetric passwords, which allows one password to be used for incoming TCP segments and a different password to be used for outgoing TCP segments.
- Configure passwords so that they overlap for a period of time. This functionality is beneficial when the clocks on two LSRs are not synchronized.

These enhancements are available by using the **key-chain** command, which allows different key strings to be used at different times according to the keychain configuration.

## Keychains Use with MPLS LDP—Lossless MD5 Session Authentication

The MPLS LDP—Lossless MD5 Session Authentication feature allows keychains to be used to specify different MD5 keys to authenticate LDP traffic exchanged in each direction.

In the following example, three passwords are configured:

- Key 1 specifies the lab password. The **send-lifetime** command enables the lab password to authenticate the outgoing TCP segments from November 2, 2007, at 10:00:00 a.m. until December 2, 2007, at 10:00:00 a.m. The **accept-lifetime** command is configured so that the lab password is never used to authenticate incoming TCP segments. The **accept-lifetime** command enables the lab password for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the password for incoming TCP segments immediately expires. If the **accept-lifetime** command is omitted from the keychain configuration, then the password is always valid for incoming TCP segments.
- Key 2 and key 3 specify the lab2 and lab3 passwords, respectively. The **send-lifetime** commands enable the passwords for 1 second on January 1, 1970. By setting the date to the past and by enabling a duration of 1 second, the passwords for outgoing TCP segments immediately expire. If the **send-lifetime** commands are omitted from the keychain configuration, the passwords are always valid for outgoing TCP segments. The **accept-lifetime** commands for key 2 and key 3 enable the passwords to authenticate the incoming TCP segments from November 2, 2007, at 10:00:00 a.m. until November 17, 2007, at 10:00:00 a.m. and from November 17, 2007, at 10:00:00 a.m. until December 2, 2007, at 10:00:00 a.m., respectively.

```
key chain ldp-pwd
key 1
  key-string lab
  send-lifetime 10:00:00 Nov 2 2007 10:00:00 Dec 2 2007
  accept-lifetime 00:00:00 Jan 1 1970 duration 1
key 2
  key-string lab2
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 2 2007 10:00:00 Nov 17 2007
key 3
  key-string lab3
  send-lifetime 00:00:00 Jan 1 1970 duration 1
  accept-lifetime 10:00:00 Nov 17 2007 10:00:00 Dec 2 2007
!
mpls ldp password option 1 for nbr-acl key-chain ldp-pwd
```

## Application of Rules to Overlapping Passwords

Overlapping passwords can be useful when two LSRs have clocks that are not synchronized. The overlapping passwords provide a window to ensure that TCP packets are not dropped. The following rules apply to overlapping passwords:

- If the send-lifetime value for the next password begins before the send-lifetime value of the current password expires, the password with the shorter key ID is used during the overlap period. The send-lifetime value of the current password can be shortened by configuring a shorter send-lifetime value. Similarly, the send-lifetime value of the current password can be lengthened by configuring a longer send-lifetime value.



- If the accept-lifetime value for the next password begins before the accept-lifetime value of the current password expires, both the next password and the current password are used concurrently. The next password information is passed to TCP. If TCP fails to authenticate the incoming segments with the current password, it tries authenticating with the next password. If TCP authenticates a segment using the new password, it discards the current password and uses the new password from that point on.
- If a password for incoming or outgoing segments expires and no additional valid password is configured, one of the following actions take place:
  - If a password is required for the neighbor, LDP drops the existing session.
  - If a password is not required for the neighbor, LDP attempts to roll over to a session that does not require authentication. This attempt also fails unless the password expires on both LSRs at the same time.

## Password Rollover Period Guidelines

Both old and new passwords are valid during a rollover period. This ensures a smooth rollover when clocks are not synchronized between two LDP neighbors. When passwords are configured using a keychain, the rollover period is equal to the accept-lifetime overlap between two successive receive passwords.

The minimum rollover period (the duration between two consecutive MD5 key updates) must be longer than the value of the LDP keepalive interval time to ensure an update of new MD5 authentication keys. If LDP session hold time is configured to its default value of 3 minutes, the LDP keepalive interval is 1 minute. The minimum rollover period should be 5 minutes. However, we recommend that the minimum rollover period is set to between 15 and 30 minutes.

To ensure a seamless rollover, follow these guidelines:

- Ensure that the local time on the peer LSRs is the same before configuring the keychain.
- Check for error messages (TCP-6-BADAUTH) that indicate keychain misconfiguration.
- Validate the correct keychain configuration by checking for the following password messages:

```
%LDP-5-PWDCFG: Password configuration changed for 10.1.1.1:0
%LDP-5-PWDRO: Password rolled over for 10.1.1.1:0
```

## Resolving LDP Password Problems

LDP displays error messages when an unexpected neighbor attempts to open an LDP session, or the LDP password configuration is invalid. Some existing LDP debugs also display password information.

When a password is required for a potential LDP neighbor, but no password is configured for it, the LSR ignores LDP hello messages from that neighbor. When the LSR processes the hello message and tries to establish a TCP connection with the neighbor, it displays the error message and stops establishing the LDP session with the neighbor. The error is rate-limited and has the following format:

```
00:00:57: %LDP-5-PWD: MD5 protection is required for peer 10.2.2.2(11051), no password configured
```

When passwords do not match between LDP peers, TCP displays the following error message on the LSR that has the lower router ID; that is, the router that has the passive role in establishing TCP connections:

```
00:01:07: %TCP-6-BADAUTH: Invalid MD5 digest from 10.2.2.2(11051) to 10.1.1.1(646)
```

If one peer has a password configured and the other one does not, TCP displays the following error messages on the LSR that has a password configured:

```
00:02:07: %TCP-6-BADAUTH: No MD5 digest from 10.1.1.1(646) to 10.2.2.2(11099)
```

## How to Configure MPLS LDP—Lossless MD5 Session Authentication

This section contains the following procedures:

- [Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain, page 7](#) (Optional)
- [Enabling the Display of MPLS LDP Password Rollover Changes and Events, page 12](#) (Optional)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Passwords, page 13](#) (Optional)

## Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain

Perform this task to configure the MPLS LDP—Lossless MD5 Session Authentication feature using a keychain. Keychains allow a different key string to be used at different times according to the keychain configuration. MPLS LDP queries the appropriate keychain to obtain the current live key and key ID for the specified keychain.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list** *access-list-number* {**permit** | **deny**} {*type-code wildcard-mask* | *ip-address mask*}
4. **key chain** *name-of-chain*
5. **key** *key-id*
6. **key-string** *string*
7. **accept-lifetime** {*start-time* | **local start-time**} {**duration seconds** | *end-time* | **infinite**}
8. **send-lifetime** {*start-time* | **local start-time**} {**duration seconds** | *end-time* | **infinite**}
9. **exit**
10. **exit**
11. **mpls ldp** [**vrf** *vrf-name*] **password option number for acl** {**key-chain** *keychain-name* | [**0** | **7**] *password*}
12. **exit**
13. **show mpls ldp neighbor** [**vrf** *vrf-name* | **all**] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter the password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>access-list</b> <i>access-list-number</i> { <b>permit</b>   <b>deny</b> } { <i>type-code wildcard-mask</i>   <i>ip-address mask</i> }  <b>Example:</b> Router(config)# access-list 10 permit 10.2.2.2	Creates an access list.
Step 4	<b>key chain</b> <i>name-of-chain</i>  <b>Example:</b> Router(config)# key chain ldp-pwd	Enables authentication for routing protocols and identifies a group of authentication keys. <ul style="list-style-type: none"> <li>Enters keychain configuration mode.</li> </ul>
Step 5	<b>key</b> <i>key-id</i>  <b>Example:</b> Router(config-keychain)# key 1	Identifies an authentication key on a keychain. <ul style="list-style-type: none"> <li>The <i>key-id</i> value must be a numeral.</li> <li>Enters keychain key configuration mode.</li> </ul>
Step 6	<b>key-string</b> <i>string</i>  <b>Example:</b> Router(config-keychain-key)# key-string pwd1	Specifies the authentication string for a key. <ul style="list-style-type: none"> <li>The <i>string</i> value can be 1 to 80 uppercase or lowercase alphanumeric characters; the first character cannot be a numeral.</li> </ul>

	Command or Action	Purpose
Step 7	<p><b>accept-lifetime</b> {<i>start-time</i>   <b>local</b> <i>start-time</i>}  {<b>duration</b> <i>seconds</i>   <i>end-time</i>   <b>infinite</b>}</p> <p><b>Example:</b>  Router(config-keychain-key)# accept-lifetime 10:00:00  Jan 13 2007 10:00:00 Jan 13 2009</p>	<p>Specifies the time period during which the authentication key on a keychain can be used for verifying incoming TCP segments.</p> <p>The <i>start-time</i> argument identifies the time to start and the local <i>start-time</i> argument identifies the time to start in the local time zone. Both arguments have the same parameters:</p> <p><b>Note</b> The time reference depends on the clock time zone configuration on the router. If no time zone configured, then the default time zone uses the Coordinated Universal Time (UTC) time. If it is configured, either the Eastern Standard Time (EST) or Pacific Standard Time (PST) time zone is used.</p> <ul style="list-style-type: none"> <li>• <i>hh:mm:ss</i> is the time format.</li> <li>• Enter the number of days from 1 to 31.</li> <li>• Enter the name of the month.</li> <li>• Enter the year from the present to 2035.</li> </ul> <p>Once the start time is entered, select from the following:</p> <ul style="list-style-type: none"> <li>• The <b>duration</b> keyword sets the key lifetime duration in seconds.</li> <li>• The <i>end-time</i> argument sets the time to stop. These parameters are the same as those used for the <i>start-time</i> argument.</li> <li>• The <b>infinite</b> keyword allows the accept-lifetime period to never expire.</li> </ul> <p>If the <b>no accept-lifetime</b> value is defined, the associated receive password is valid for authenticating incoming TCP segments.</p>

Command or Action	Purpose
<p><b>Step 8</b></p> <pre>send-lifetime {start-time   local start-time} {duration seconds   end-time   infinite}</pre> <p><b>Example:</b>  Router(config-keychain-key)# send-lifetime 10:00:00  Jan 13 2007 10:00:00 Jan 13 2009</p>	<p>Specifies the time period during which the authentication key on a keychain can be used for verifying outgoing TCP segments. The <i>start-time</i> argument identifies the time to start and the local <i>start-time</i> argument identifies the time to start in the local time zone. Both arguments have the same parameters:</p> <p><b>Note</b> The time reference depends on the clock time zone configuration on the router. If no time zone configured, then the default time zone uses the UTC time. If it is configured, either the EST or PST time zone is used.</p> <ul style="list-style-type: none"> <li>• <i>hh:mm:ss</i> is the time format.</li> <li>• Enter the number of days from 1 to 31.</li> <li>• Enter the name of the month.</li> <li>• Enter the year from 1993 to 2035.</li> </ul> <p>Once the start time is entered, select from the following:</p> <ul style="list-style-type: none"> <li>• The <b>duration</b> keyword sets the send lifetime duration in seconds.</li> <li>• The <i>end-time</i> argument sets the time to stop. These parameters are the same as those used for the <i>start-time</i> argument.</li> <li>• The <b>infinite</b> keyword allows the send lifetime period to never expire.</li> </ul> <p>If the <b>no send-lifetime</b> value is defined, the associated send password is valid for authenticating outgoing TCP segments.</p>
<p><b>Step 9</b></p> <pre>exit</pre> <p><b>Example:</b>  Router(config-keychain-key)# exit</p>	<p>Exits from keychain key configuration mode.</p>
<p><b>Step 10</b></p> <pre>exit</pre> <p><b>Example:</b>  Router(config-keychain)# exit</p>	<p>Exits from keychain configuration mode.</p>

	Command or Action	Purpose
<b>Step 11</b>	<p><b>mpls ldp</b> [<b>vrf</b> <i>vrf-name</i>] <b>password</b> <b>option</b> <i>number</i> <b>for</b> <i>acl</i> {<b>key-chain</b> <i>keychain-name</i>   [<b>0</b>   <b>7</b>] <i>password</i>}</p> <p><b>Example:</b></p> <pre>Router(config)# mpls ldp password option 1 for 10 keychain ldp-pwd</pre>	<p>Configures an MD5 password for LDP sessions with neighbors whose LDP router IDs are permitted by a specified access list.</p> <ul style="list-style-type: none"> <li>• The <b>vrf</b> <i>vrf-name</i> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>• The <i>number</i> argument defines the order in which the access lists are evaluated in the determination of a neighbor password. The valid range is 1 to 32767.</li> <li>• The <b>for</b> <i>acl</i> keyword-argument pair specifies the name of the access list that includes the LDP router IDs of those neighbors for which the password applies. Only standard IP access list values (1 to 99) can be used for the <i>acl</i> argument.</li> <li>• The <b>key-chain</b> <i>keychain-name</i> keyword-argument pair specifies the name of the keychain to use.</li> <li>• The <b>0</b> and <b>7</b> keywords specify whether the password that follows is hidden (encrypted); <ul style="list-style-type: none"> <li>– <b>0</b> specifies an unencrypted password.</li> <li>– <b>7</b> specifies an encrypted password.</li> </ul> </li> <li>• The <i>password</i> argument specifies the MD5 password to be used for the specified LDP sessions.</li> </ul>

	Command or Action	Purpose
Step 12	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits from global configuration mode.
Step 13	<b>show mpls ldp neighbor</b> [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ] [ <i>ip-address</i>   <i>interface</i> ] [ <b>detail</b> ] [ <b>graceful-restart</b> ]  <b>Example:</b> Router# show mpls ldp neighbor detail	Displays the status of LDP sessions. <ul style="list-style-type: none"> <li>• The <b>vrf</b> <i>vrf-name</i> keyword-argument pair displays the LDP neighbors for the specified VRF instance.</li> <li>• The <i>ip-address</i> argument identifies the neighbor with the IP address for which password protection is configured.</li> <li>• The <i>interface</i> argument identifies the LDP neighbors accessible over this interface.</li> <li>• The <b>detail</b> keyword displays information in long form, including password information for this neighbor. Here are the items displayed: <ul style="list-style-type: none"> <li>– An indication as to whether a password is mandatory for this neighbor (required/not required)</li> <li>– The password source (neighbor/fallback/number [option number])</li> <li>– An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale)</li> </ul> </li> <li>• The <b>graceful-restart</b> keyword displays per-neighbor graceful restart information.</li> </ul>

## Enabling the Display of MPLS LDP Password Rollover Changes and Events

When a password is required for a neighbor, but no password is configured for the neighbor, the following debug message is displayed:

```
00:05:04: MDSym5 protection is required for peer 10.2.2.2:0(glbl), but no password configured.
```

To enable the display of events related to configuration changes and password rollover events, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp logging password configuration** [**rate-limit** *number*]
4. **mpls ldp logging password rollover** [**rate-limit** *number*]



5. **exit**
6. **debug mpls ldp transport events**  
or  
**debug mpls ldp transport connections**

## DETAILED STEPS

- 
- Step 1 enable**  
This command enables privileged EXEC mode. Enter the password if prompted.
- Step 2 configure terminal**  
This command enables global configuration mode.
- Step 3 mpls ldp logging password configuration [rate-limit *number*]**  
This command is used to enable the display of events related to configuration changes. The output displays events when a new password is configured or an existing password has been changed or deleted. A rate limit of 1 to 60 messages a minute can be specified.
- Step 4 mpls ldp logging password rollover [rate-limit *number*]**  
This command is used to enable the display of events related to password rollover events. Events are displayed when a new password is used for authentication or when authentication is disabled. A rate limit of 1 to 60 messages a minute can be specified.
- Step 5 exit**  
This command exits global configuration mode.
- Step 6 debug mpls ldp transport events**  
or  
**debug mpls ldp transport connections**  
Either command displays notifications when a session TCP MD5 option is changed.  
For example:
- ```
00:03:44: ldp: MD5 setup for peer 10.2.2.2:0(global); password changed to adfas
00:05:04: ldp: MD5 setup for peer 10.52.52.2:0(vpn1(1)); password changed to [nil]
```
- 

## Changing MPLS LDP—Lossless MD5 Session Authentication Passwords

The MPLS LDP—Lossless MD5 Session Authentication feature allows MD5 passwords to be changed for LDP session authentication without having to close and reestablish an existing LDP session.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp [vrf *vrf-name*] password rollover duration *minutes***
4. **mpls ldp [vrf *vrf-name*] password fallback {key-chain *keychain-name* | [0 | 7] *password*}**
5. **no mpls ldp neighbor [vrf *vpn-name*] ip-address *password password***

6. **exit**

7. **show mpls ldp neighbor** [**vrf** *vrf-name*] [*ip-address* | *interface*] [**detail**] [**graceful-restart**]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter the password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>mpls ldp</b> [ <b>vrf</b> <i>vrf-name</i> ] <b>password rollover</b> <i>duration</i> <i>minutes</i><br><br><b>Example:</b><br>Router(config)# mpls ldp password rollover duration 7                                                              | Configures the duration before the new password takes effect. <ul style="list-style-type: none"> <li>The <b>vrf</b> <i>vrf-name</i> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>The <i>minutes</i> argument specifies the number of minutes from 5 to 65535 before the password rollover occurs on this router.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 4 | <b>mpls ldp</b> [ <b>vrf</b> <i>vrf-name</i> ] <b>password fallback</b> { <b>key-chain</b> <i>keychain-name</i>   [ <b>0</b>   <b>7</b> ] <i>password</i> }<br><br><b>Example:</b><br>Router(config)# mpls ldp password fallback key-chain fallback | Configures an MD5 password for LDP sessions with peers. <ul style="list-style-type: none"> <li>The <b>vrf</b> <i>vrf-name</i> keyword-argument pair specifies a VRF configured on the LSR.</li> <li>The <b>key-chain</b> <i>keychain-name</i> keyword-argument pair specifies the name of the keychain used to specify the MD5 key that authenticates the exchange of bidirectional LDP traffic.</li> <li>The <b>0</b> and <b>7</b> keywords specify whether the password that follows is hidden (encrypted); <ul style="list-style-type: none"> <li><b>0</b> specifies an unencrypted password.</li> <li><b>7</b> specifies an encrypted password.</li> </ul> </li> <li>The <i>password</i> argument specifies the MD5 password to be used for the specified LDP sessions.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>no mpls ldp neighbor</b> [<b>vrf</b> <i>vpn-name</i>] <i>ip-address</i><br/> <b>password</b> <i>password</i></p> <p><b>Example:</b><br/> Router(config)# no mpls ldp neighbor 10.11.11.11<br/> password lab1</p> | <p>Disables the configuration of a password for computing MD5 checksums for the session TCP connection with the specified neighbor.</p> <ul style="list-style-type: none"> <li>• The <b>vrf</b> <i>vpn-name</i> argument optionally specifies the VRF instance for the specified neighbor.</li> <li>• The <i>ip-address</i> argument identifies the neighbor router ID.</li> <li>• The <b>password</b> <i>password</i> keyword-argument pair is necessary so that the router computes MD5 checksums for the session TCP connection with the specified neighbor.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 6 | <p><b>exit</b></p> <p><b>Example:</b><br/> Router(config)# exit</p>                                                                                                                                                    | <p>Exits from global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 7 | <p><b>show mpls ldp neighbor</b> [<b>vrf</b> <i>vrf-name</i>] [<i>ip-address</i>   <i>interface</i>] [<b>detail</b>] [<b>graceful-restart</b>]</p> <p><b>Example:</b><br/> Router# show mpls ldp neighbor detail</p>   | <p>Displays the status of LDP sessions.</p> <ul style="list-style-type: none"> <li>• The <b>vrf</b> <i>vrf-name</i> keyword-argument pair displays the LDP neighbors for the specified VRF instance.</li> <li>• The <i>ip-address</i> argument identifies the neighbor with the IP address for which password protection is configured.</li> <li>• The <i>interface</i> argument lists the LDP neighbors accessible over this interface.</li> <li>• The <b>detail</b> keyword displays information in long form, including password information for this neighbor. Here are the items displayed: <ul style="list-style-type: none"> <li>– An indication as to whether a password is mandatory for this neighbor (required/not required)</li> <li>– The password source (neighbor/fallback/number [option number])</li> <li>– An indication as to whether the latest configured password for this neighbor is used by the TCP session (in use) or the TCP session uses an old password (stale)</li> </ul> </li> <li>• The <b>graceful-restart</b> keyword displays per-neighbor graceful restart information.</li> </ul> |

# Configuration Examples for MPLS LDP—Lossless MD5 Session Authentication

This section provides the following configuration examples:

- [Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain \(Symmetrical\): Example, page 16](#)
- [Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain \(Asymmetrical\): Example, page 17](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Password: Example, page 18](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Rollover Without Keychain: Example, page 19](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Rollover with a Keychain: Example, page 20](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Fallback Password With a Keychain: Example, page 22](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication: Common Misconfiguration Examples, page 24](#)
- [Changing MPLS LDP—Lossless MD5 Session Authentication Using a Second Key to Avoid LDP Session Failure: Examples, page 26](#)

## Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain (Symmetrical): Example

The following example shows a configuration of two peer LSRs that use symmetrical MD5 keys:

### LSR1

```
access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
key 1
  key-string pwd1
  send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
  accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
!
interface loopback0
  ip address 10.1.1.1 255.255.255.255
!
interface Ethernet0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  tag-switching ip
```

### LSR2

```
access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
```

```

key chain ldp-pwd
  key 1
    key-string pwd1
    send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
    accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
  !
interface loopback0
  ip address 10.2.2.2 255.255.255.255
  !
interface Ethernet0/0
  ip address 10.0.1.2 255.255.255.254
  mpls label protocol ldp
  tag-switching ip

```

## Configuring MPLS LDP—Lossless MD5 Session Authentication Using a Keychain (Asymmetrical): Example

The following example shows a configuration of two peer LSRs that use asymmetrical MD5 keys:

### LSR1

```

access-list 10 permit 10.2.2.2
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
  key 1
    key-string pwd1
    accept-lifetime 00:00:00 Jan 1 2005 duration 1
    send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
  key 2
    key-string pwd2
    accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
    send-lifetime 00:00:00 Jan 1 2005 duration 1
  !
interface loopback0
  ip address 10.1.1.1 255.255.255.255
  !
interface Ethernet0/0
  ip address 10.0.1.1 255.255.255.254
  mpls label protocol ldp
  tag-switching ip

```

### LSR2

```

access-list 10 permit 10.1.1.1
mpls ldp password required for 10
mpls ldp password option 1 for 10 ldp-pwd
!
key chain ldp-pwd
  key 1
    key-string pwd2
    accept-lifetime 00:00:00 Jan 1 2005 duration 1
    send-lifetime 10:00:00 Jan 1 2007 10:00:00 Feb 1 2007
  key 2
    key-string pwd1
    accept-lifetime 09:00:00 Jan 1 2007 11:00:00 Feb 1 2007
    send-lifetime 00:00:00 Jan 1 2005 duration 1
  !
interface loopback0
  ip address 10.2.2.2 255.255.255.255

```

```

!
interface Ethernet0/0
 ip address 10.0.1.2 255.255.255.254
 mpls label protocol ldp
 tag-switching ip

```

## Changing MPLS LDP—Lossless MD5 Session Authentication Password: Example

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

### LSR A Existing Configuration

```

mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls ldp neighbor 10.12.12.12 password lab1
mpls label protocol ldp
!
interface loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
 ip address 10.2.0.1 255.255.0.0
 mpls ip
!
interface Ethernet2/0
 ip address 10.0.0.1 255.255.0.0
 mpls ip

```

### LSR B Existing Configuration

```

mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
 ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
 ip address 10.2.0.2 255.255.0.0
 mpls ip

```

### LSR C Existing Configuration

```

mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
 ip address 10.12.12.12 255.255.255.255
!
interface Ethernet2/0
 ip address 10.0.0.2 255.255.0.0
 mpls ip
!

```

The following example shows how the lossless password change is configured using the **mpls ldp password rollover duration** command for LSR A, LSR B, and LSR C so there is enough time to change all the passwords on all of the routers:

#### LSR A New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1
```

#### LSR B New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

#### LSR C New Configuration

```
mpls ldp password rollover duration 10
mpls ldp password fallback lab2
no mpls ldp neighbor 10.10.10.10 password lab1
```

After 10 minutes has elapsed, the password changes. The following system logging message for LSR A confirms that the password rollover was successful:

```
%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0
```

## Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Rollover Without Keychain: Example

The MPLS LDP—Lossless MD5 Session Authentication password can be changed in a lossless way (without tearing down an existing LDP session) by using a password rollover without a keychain.

The following example shows the existing password configuration for LSR A and LSR B:

#### LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls ldp neighbor 10.11.11.11 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.1 255.255.0.0
mpls ip
```

**LSR B Existing Configuration**

```

mpls ldp router-id loopback0 force
mpls ldp neighbor 10.10.10.10 password lab1
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.2 255.255.0.0
mpls ip

```

The following example shows the new password configuration for LSR A and LSR B:

**Note**

The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

**LSR A New Configuration**

```

mpls ldp password rollover duration 10
mpls ldp neighbor 10.11.11.11 password lab2

```

**LSR B New Configuration**

```

mpls ldp password rollover duration 10
mpls ldp neighbor 10.10.10.10 password lab2

```

After 10 minutes (rollover duration), the password changes and the following system logging message confirms the password rollover at LSR A:

```
%LDP-5-PWDR0: Password rolled over for 10.11.11.11:0
```

## Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Rollover with a Keychain: Example

The MPLS LDP—Lossless MD5 Session Authentication password can be changed in a lossless way by using a password rollover with a keychain. The following configuration example shows the new password keychain configuration for LSR A, LSR B, and LSR C, in which the new password is ldp-pwd.

In the example, the desired keychain is configured first. The first pair of keys authenticate incoming TCP segments (recv key) and compute MD5 digests for outgoing TCP segments (xmit key). These keys should be the same keys as those currently in use; that is, in lab 1. The second recv key in the keychain should be valid after a few minutes. The second xmit key becomes valid at a future time.

**Note**

The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

**LSR A New Configuration**

```

mpls ldp password rollover duration 10
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1

```



```

send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
    key 11
    key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
    key 12
    key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.11.11.11 password lab1
no mpls ldp neighbor 10.12.12.12 password lab1

```

### LSR B New Configuration

```

mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
    key chain ldp-pwd
    key 10
    key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
    key 11
    key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
    key 12
    key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1

```

### LSR C New Configuration

```

mpls ldp password rollover duration 10
access-list 10 permit 10.10.10.10
    key chain ldp-pwd
    key 10
    key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
    key 11
    key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
    key 12
    key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
no mpls ldp neighbor 10.10.10.10 password lab1

```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A.

```

%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0

```

## Changing MPLS LDP—Lossless MD5 Session Authentication Password Using a Fallback Password With a Keychain: Example

The MPLS LDP—Lossless MD5 Session Authentication password can be changed in a lossless way by using a fallback password when doing a rollover with a keychain.



### Note

The fallback password is used only when there is no other keychain configured. If there is a keychain configured, then the fallback password is not used.

The following example shows the existing password configuration for LSR A, LSR B, and LSR C:

### LSR A Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.10.10.10 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.1 255.255.0.0
mpls ip
!
interface Ethernet2/0
ip address 10.0.0.1 255.255.0.0
mpls ip
!
access-list 10 permit 10.11.11.11
access-list 10 permit 10.12.12.12
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

### LSR B Existing Configuration

```
mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.11.11.11 255.255.255.255
!
interface Ethernet1/0
ip address 10.2.0.2 255.255.0.0
mpls ip
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

**LSR C Existing Configuration**

```

mpls ldp router-id loopback0 force
mpls label protocol ldp
!
interface loopback0
ip address 10.12.12.12 255.255.255.255
!
interface Ethernet2/0
ip address 10.0.0.2 255.255.0.0
mpls ip
!
access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd

```

**Note**

The fallback keychain is not used unless the keychain **ldp-pwd** is removed using the **no mpls ldp password option 5 for 10 key-chain ldp-pwd** command.

The following example shows the new configuration for LSR A, LSR B, and LSR C, where one keychain is configured with the name **ldp-pwd** and another keychain is configured with the name **fallback** for the fallback password.

**Note**

The rollover duration should be large enough so that the passwords can be changed on all impacted routers.

**LSR A New Configuration**

```

mpls ldp password rollover duration 10
!
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd

```

**LSR B New Configuration**

```

mpls ldp password rollover duration 10
!
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd

```

**LSR C New Configuration**

```

mpls ldp password rollover duration 10
key chain fallback
key 10
key-string fbk1
!
mpls ldp password fallback key-chain fallback
!
no mpls ldp password option 5 for 10 key-chain ldp-pwd

```

After 10 minutes, the password changes and the following system logging message confirms the password rollover at LSR A:

```

%LDP-5-PWDRO: Password rolled over for 10.11.11.11:0
%LDP-5-PWDRO: Password rolled over for 10.12.12.12:0

```

## Changing MPLS LDP—Lossless MD5 Session Authentication: Common Misconfiguration Examples

The following sections describe common misconfiguration examples that can occur when the MPLS LDP—Lossless MD5 Session Authentication password is migrated in a lossless way. Misconfigurations can lead to undesired behavior in an LDP session.

- [Incorrect Keychain LDP Password Configuration: Example, page 24](#)
- [Avoiding Access List Configuration Problems, page 26](#)

### Incorrect Keychain LDP Password Configuration: Example

Possible misconfigurations can occur when keychain-based commands are used with the **mpls ldp password option for key-chain** command. If the **accept-lifetime** or **send-lifetime** command is not specified in this configuration, then a misconfiguration can occur when more than two keys are in a keychain.

The following example shows an incorrect keychain configuration with three passwords for LSR A and LSR B in the keychain:

**LSR A Incorrect Keychain LDP Password Configuration**

```

access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd

```

**LSR B Incorrect Keychain LDP Password Configuration**

```

access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd

```

In the example, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007** command, all three configured keys are valid as receive keys, and only the last configured key is valid as a transmit key. The keychain resolution rules dictate that keys 10 and 11 are used as receive keys, and only the last key 12 can be used as the transmit key. Because the transmit and receive keys are mismatched, the LDP session will not stay active.

**Note**

When more than two passwords are configured in a keychain, the configuration needs to have both **accept-lifetime** and **send-lifetime** commands configured correctly for effective rollovers.

The following example shows the correct keychain configuration with multiple passwords in the keychain:

**LSR A Correct Keychain LDP Password Configuration**

```

access-list 10 permit 10.11.11.11
!
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd

```

**LSR B Correct Keychain LDP Password Configuration**

```

access-list 10 permit 10.10.10.10
key chain ldp-pwd
key 10
key-string lab1
send-lifetime 10:00:00 Jan 1 2007 10:30:00 Jan 1 2007
accept-lifetime 10:00:00 Jan 1 2007 10:45:00 Jan 1 2007
key 11
key-string lab2
send-lifetime 10:30:00 Jan 1 2007 10:30:00 Feb 1 2007
accept-lifetime 10:15:00 Jan 1 2007 10:45:00 Feb 1 2007
key 12

```

```
key-string lab3
send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007
accept-lifetime 10:15:00 Feb 1 2007 10:45:00 Mar 1 2007
!
mpls ldp password option 5 for 10 key-chain ldp-pwd
```

In the example above, for both LSR A and LSR B, during the period of the third **send-lifetime 10:30:00 Feb 1 2007 10:30:00 Mar 1 2007** command, only the last key 12 is valid as transmit and receive keys. Therefore, the LDP session remains active.

## Avoiding Access List Configuration Problems

Use caution when modifying or deleting an access list. Any empty access list implies "permit any" by default. So when either the **mpls ldp password option for key-chain** command or the **mpls ldp password option for** command is used for MPLS LDP MD5 session authentication, if the access list specified in the command becomes empty as a result of a modification or deletion, then all LDP sessions on the router expect a password. This configuration may cause undesired behavior in LDP sessions. To avoid this scenario, ensure that the proper access list is specified for each LSR.

## Changing MPLS LDP—Lossless MD5 Session Authentication Using a Second Key to Avoid LDP Session Failure: Examples

The MPLS LDP—Lossless MD5 Session Authentication feature works when a specified rollover period is configured. Typically, one rollover period overlaps the two accept lifetime values that are configured for two consecutive receive keys. The LDP process requests an update from the keychain manager for the latest valid transmit and receive keys once every minute. LDP compares the latest key set with the keys from the previous update in its database to determine if a key was removed, changed, or rolled over. When the rollover occurs, the LDP process detects the rollover and programs TCP with the next receive key.

The LDP session can fail if LDP is configured to use two keys for the MPLS LDP—Lossless MD5 Session Authentication feature where the first key uses a send and accept lifetime value and the second key is not configured. The configuration creates a special case where there are two rollovers but there is only one rollover period.

The following sections provide an example of this problem and a solution:

- [TCP Authentication and LDP Sessions Can Fail When a Second Rollover Period Is Missing: Example, page 27](#)
- [Reconfigure a Keychain to Prevent TCP Authentication and LDP Session Failures: Example, page 27](#)

## TCP Authentication and LDP Sessions Can Fail When a Second Rollover Period Is Missing: Example

In the following configuration, the first rollover is from “secondpass” to “firstpass.” The second rollover is from “firstpass” back to “secondpass.” The only rollover period in this configuration is the overlapping between the “firstpass” and “secondpass.” Because one rollover period is missing, LDP performs only the first rollover and not the second rollover, causing TCP authentication to fail and the LDP session to fail.

```
key chain ldp-pwd
key 1
  key-string firstpass
  accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
  send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
key 2
  key-string secondpass
```

TCP authentication and LDP sessions can also fail if the second key has send and accept lifetime configured. In this case the accept lifetime of the first key is a subset of the accept lifetime of the second key. For example:

```
key chain ldp-pwd
key 1
  key-string firstpass
  accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
  send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
key 2
  key-string secondpass
  accept-lifetime 01:03:00 Sep 9 2007 01:10:00 Sep 11 2007
  send-lifetime 01:05:00 Sep 9 2007 01:08:00 Sep 11 2007
```

## Reconfigure a Keychain to Prevent TCP Authentication and LDP Session Failures: Example

If the configuration needs to specify the last key in the keychain to always be valid, then configure the keychain to have at least two keys. Each key must be configured with both the send and accept lifetime period. For example:

```
key chain ldp-pwd
key 1
  key-string firstpass
  accept-lifetime 01:03:00 Sep 10 2007 01:10:00 Sep 10 2007
  send-lifetime 01:05:00 Sep 10 2007 01:08:00 Sep 10 2007
key 2
  key-string secondpass
  accept-lifetime 01:06:00 Sep 10 2007 01:17:00 Sep 10 2007
  send-lifetime 01:08:00 Sep 10 2007 01:15:00 Sep 10 2007
key 3
  key-string thirdpass
```

If the configuration needs to specify the first keychain for the time interval, then switch to use the second key forever after that interval. This is done by configuring the start time for the second key to begin shortly before the end time of the first key, and by configuring the second key to be valid forever after that interval. For example:

```
key chain ldp-pwd
key 1
  key-string firstpass
  accept-lifetime 00:03:00 Sep 10 2007 01:10:00 Sep 10 2007
  send-lifetime 00:05:00 Sep 10 2007 01:08:00 Sep 10 2007
key 2
  key-string secondpass
  accept-lifetime 01:06:00 Sep 10 2007 infinite
  send-lifetime 01:08:00 Sep 10 2007 infinite
```

If the configuration needs to specify the two keys in the order of the second key, first key, and second key again, then specify three keys in that order with the proper rollover period. For example:

```
key chain ldp-pwd
key 1
  key-string firstpass
  accept-lifetime 00:03:00 Sep 10 2007 01:10:00 Sep 10 2007
  send-lifetime 00:05:00 Sep 10 2007 01:08:00 Sep 10 2007
key 2
  key-string secondpass
  accept-lifetime 01:06:00 Sep 10 2007 01:17:00 Sep 10 2007
  send-lifetime 01:08:00 Sep 10 2007 01:15:00 Sep 10 2007
key 3
  key-string firstpass
  accept-lifetime 01:13:00 Sep 10 2007 infinite
  send-lifetime 01:15:00 Sep 10 2007 infinite
```



# Additional References

The following sections provide references related to the MPLS LDP—Lossless MD5 Session Authentication feature.

## Related Documents

| Related Topic                                        | Document Title                                    |
|------------------------------------------------------|---------------------------------------------------|
| MPLS Label Distribution Protocol (LDP)               | <a href="#">MPLS Label Distribution Protocol</a>  |
| LDP implementation enhancements for the MD5 password | <a href="#">MPLS LDP MD5 Global Configuration</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this release. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- **mpls ldp logging password configuration**
- **mpls ldp logging password rollover**
- **mpls ldp neighbor password**
- **mpls ldp password fallback**
- **mpls ldp password option**
- **mpls ldp password required**
- **mpls ldp password rollover duration**
- **show mpls ldp discovery**
- **show mpls ldp neighbor**
- **show mpls ldp neighbor password**

# Feature Information for MPLS LDP—Lossless MD5 Session Authentication

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS LDP—Lossless MD5 Session Authentication

| Feature Name                                 | Releases                                            | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------|-----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP—Lossless MD5 Session Authentication | 12.0(33)S<br>12.2(33)SRC<br>12.2(33)SB<br>12.4(20)T | <p>This feature allows an LDP session to be password-protected without tearing down and reestablishing the LDP session.</p> <p>This feature was introduced in Cisco IOS Release 12.0(33)S.</p> <ul style="list-style-type: none"> <li>The following commands were introduced or modified: <b>mpls ldp logging password configuration</b>, <b>mpls ldp logging password rollover</b>, <b>mpls ldp neighbor password</b>, <b>mpls ldp password fallback</b>, <b>mpls ldp password option</b>, <b>mpls ldp password required</b>, <b>mpls ldp password rollover duration</b>, <b>show mpls ldp discovery</b>, <b>show mpls ldp neighbor</b>, <b>show mpls ldp neighbor password</b>.</li> </ul> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRC.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

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



# MPLS LDP Inbound Label Binding Filtering

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) supports inbound label binding filtering. You can use the MPLS LDP feature to configure access control lists (ACLs) for controlling the label bindings a label switch router (LSR) accepts from its peer LSRs.

## History for the MPLS LDP Inbound Label Binding Filtering Feature

| Release     | Modification                                                                                     |
|-------------|--------------------------------------------------------------------------------------------------|
| 12.0(26)S   | This feature was introduced.                                                                     |
| 12.2(25)S   | This feature was integrated into Cisco IOS Release 12.2(25)S for the Cisco 7500 series router.   |
| 12.3(14)T   | This feature was integrated into Cisco IOS Release 12.3(14)T.                                    |
| 12.2(18)SXE | This feature was integrated into Cisco IOS Release 12.2(18)SXE for the Cisco 7600 series router. |

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Information about MPLS LDP Inbound Label Binding Filtering, page 2](#)
- [How to Configure MPLS LDP Inbound Label Binding Filtering, page 2](#)
- [Configuration Examples for MPLS LDP Inbound Label Binding Filtering, page 5](#)
- [Additional References, page 5](#)
- [Command Reference, page 6](#)
- [Glossary, page 8](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

# Information about MPLS LDP Inbound Label Binding Filtering

The MPLS LDP Inbound Label Binding Filtering feature may be used to control the amount of memory used to store LDP label bindings advertised by other routers. For example, in a simple MPLS Virtual Private Network (VPN) environment, the VPN provider edge (PE) routers may require LSPs only to their peer PE routers (that is, they do not need LSPs to core routers). Inbound label binding filtering enables a PE router to accept labels only from other PE routers.

## How to Configure MPLS LDP Inbound Label Binding Filtering

This section includes the following tasks:

- [Configuring MPLS LDP Inbound Label Binding Filtering, page 2](#) (Required)
- [Verifying that MPLS LDP Inbound Label Bindings are Filtered, page 4](#) (Optional)

## Configuring MPLS LDP Inbound Label Binding Filtering

Perform this task to configure a router for inbound label filtering. The following configuration allows the router to accept only the label for prefix 25.0.0.2 from LDP neighbor router 10.12.12.12.

### Restrictions

Inbound label binding filtering does not support extended ACLs; it only supports standard ACLs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip access-list standard** *access-list-number*
4. **permit** {*source* [*source-wildcard*] | **any**} [**log**]
5. **exit**
6. **mpls ldp neighbor** [*vrf vpn-name*] *nbr-address* **labels accept** *acl*
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip access-list standard access-list-number</b><br><br><b>Example:</b><br>Router(config)# ip access-list standard 1                                         | Defines a standard IP access list with a number.                                                                 |
| Step 4 | <b>permit {source [source-wildcard]   any} [log]</b><br><br><b>Example:</b><br>Router(config-std-nacl)# permit 10.0.0.0                                       | Specifies one or more prefixes permitted by the access list.                                                     |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-std-nacl)# exit                                                                                           | Exits the current mode and goes to the next higher level.                                                        |
| Step 6 | <b>mpls ldp neighbor [vrf vpn-name] nbr-address labels accept acl</b><br><br><b>Example:</b><br>Router(config)# mpls ldp neighbor 10.12.12.12 labels accept 1 | Specifies the ACL to be used to filter label bindings for the specified LDP neighbor.                            |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                      | Exits the current mode and enters privileged Exec mode.                                                          |

## Verifying that MPLS LDP Inbound Label Bindings are Filtered

If inbound filtering is enabled, perform the following steps to verify that inbound label bindings are filtered:

- Step 1** Enter the **show mpls ldp neighbor** command to show the status of the LDP session, including the name or number of the ACL configured for inbound filtering.

```
show mpls ldp neighbor [vrf vpn-name][address | interface] [detail]
```



**Note** To display information about inbound label binding filtering, you must enter the **detail** keyword.

Following is sample output from the **show mpls ldp neighbor** command.

```
Router# show mpls ldp neighbor 10.12.12.12 detail

Peer LDP Ident: 10.12.12.12:0; Local LDP Ident 10.13.13.13:0
TCP connection: 10.12.12.12.646 - 10.13.13.13.12592
State: Oper; Msgs sent/rcvd: 49/45; Downstream; Last TIB rev sent 1257
Up time: 00:32:41; UID: 1015; Peer Id 0;
LDP discovery sources:
  Serial1/0; Src IP addr: 25.0.0.2
    holdtime: 15000 ms, hello interval: 5000 ms
Addresses bound to peer LDP Ident:
  10.0.0.129      10.12.12.12      10.0.0.2
Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
LDP inbound filtering accept acl: 1
```

- Step 2** Enter the **show ip access-list** command to display the contents of all current IP access lists or of a specified access list.

```
show ip access-list [access-list-number | access-list-name]
```



**Note** It is important that you enter this command to see how the access list is defined; otherwise, you cannot verify inbound label binding filtering.

*The following command output shows the contents of IP access list 1:*

```
Router# show ip access 1

Standard IP access list 1
  permit 10.0.0.0, wildcard bits 0.0.0.255 (1 match)
```

- Step 3** Enter the **show mpls ldp bindings** command to verify that the LSR has remote bindings only from a specified peer for prefixes permitted by the access list.

```
Router# show mpls ldp bindings

tib entry: 10.0.0.0/8, rev 4
  local binding: tag: imp-null
tib entry: 10.2.0.0/16, rev 1137
  local binding: tag: 16
tib entry: 10.2.0.0/16, rev 1139
  local binding: tag: 17
tib entry: 10.12.12.12/32, rev 1257
  local binding: tag: 18
tib entry: 10.13.13.13/32, rev 14
  local binding: tag: imp-null
```



```
tib entry: 10.10.0.0/16, rev 711
    local binding: tag: imp-null
tib entry: 10.0.0.0/8, rev 1135
    local binding: tag: imp-null
    remote binding: tsr: 12.12.12.12:0, tag: imp-null
tib entry: 10.0.0.0/8, rev 8
    local binding: tag: imp-null
Router#
```

---

## Configuration Examples for MPLS LDP Inbound Label Binding Filtering

In the following example, the **mpls ldp neighbor labels accept** command is configured with an access control list to filter label bindings received on sessions with the neighbor 10.110.0.10.

Label bindings for prefixes that match 10.b.c.d are accepted, where b is less than or equal to 63, and c and d can be any integer between 0 and 128. Other label bindings received from 10.110.0.10 are rejected.

```
Router# configure terminal
Router(config)# access-list 1 permit 10.63.0.0 0.63.255.255
Router(config)# mpls ldp neighbor 10.110.0.10 labels accept 1
Router(config)# end
```

In the following example, the **show mpls ldp bindings neighbor** command displays label bindings that were learned from 10.110.0.10. This example verifies that the LIB does not contain label bindings for prefixes that have been excluded.

```
Router# show mpls ldp bindings neighbor 10.110.0.10

tib entry: 10.2.0.0/16, rev 4
    remote binding: tsr: 10.110.0.10:0, tag: imp-null
tib entry: 10.43.0.0/16, rev 6
    remote binding: tsr: 10.110.0.10:0, tag: 16
tib entry: 10.52.0.0/16, rev 8
    remote binding: tsr: 10.110.0.10:0, tag: imp-null
```

## Additional References

The following sections provide additional references related to MPLS LDP inbound label binding filters.

## Related Documents

| Related Topic                          | Document Title                                   |
|----------------------------------------|--------------------------------------------------|
| MPLS Label Distribution Protocol (LDP) | <a href="#">MPLS Label Distribution Protocol</a> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                                                  | MIBs Link                                                                                                                                                                                                              |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>LDP Specification, draft-ietf-mpls-ldp-08.txt</i> | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                             |
|----------|-----------------------------------|
| RFC 3036 | <a href="#">LDP Specification</a> |
| RFC 3037 | <a href="#">LDP Applicability</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                         | Link                                                                            |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- `clear mpls ldp neighbor`

- **mpls ldp neighbor labels accept**
- **show mpls ldp neighbor**

# Glossary

**carrier supporting carrier**—A situation where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

**inbound label binding filtering**—Allows LSRs to control which label bindings it will accept from its neighboring LSRs. Consequently, an LSR does not accept or store some label bindings that its neighbors advertise.

**label**—A short fixed-length identifier that tells switching nodes how to forward data (packets or cells).

**label binding**—An association between a destination prefix and a label.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS LDP—Local Label Allocation Filtering

---

**First Published: January 7, 2008**

**Last Updated: April 11, 2008**

This feature introduces command-line interface (CLI) commands to modify the way in which Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation. This MPLS LDP feature enhancement enables the configuration of filtering policies for selective local label binding assignments by LDP to improve LDP scalability and convergence.

This document contains information about and instructions on how to configure the MPLS LDP—Local Label Allocation Filtering feature.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS LDP—Local Label Allocation Filtering](#)” section on page 19.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS LDP—Local Label Allocation Filtering](#), page 2
- [Restrictions for MPLS LDP—Local Label Allocation Filtering](#), page 2
- [Information About MPLS LDP—Local Label Allocation Filtering](#), page 2
- [How to Configure MPLS LDP—Local Label Allocation Filtering](#), page 5
- [Configuration Examples for MPLS LDP—Local Label Allocation Filtering](#), page 10
- [Additional References](#), page 17
- [Command Reference](#), page 18



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Feature Information for MPLS LDP—Local Label Allocation Filtering, page 19](#)
- [Glossary, page 21](#)

## Prerequisites for MPLS LDP—Local Label Allocation Filtering

The MPLS LDP—Local Label Allocation Filtering feature requires the MPLS Forwarding Infrastructure (MFI).

## Restrictions for MPLS LDP—Local Label Allocation Filtering

The MPLS LDP—Local Label Allocation Filtering feature does not support access lists. This feature supports prefix lists.

Restrictions for the MPLS LDP—Local Label Allocation Filtering feature in Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB:

- LDP local label allocation configuration for prefix list or host routes is supported only in the global routing table.
- LDP and RIB restart handling supported in Cisco IOX software does not apply.
- Wildcard Forwarding Equivalence Class (FEC) requests are not supported.
- Remote bindings are retained for LDP table entries that are filtered.

## Information About MPLS LDP—Local Label Allocation Filtering

Before you configure the MPLS LDP—Local Label Allocation Filtering feature, you should understand the following concepts:

- [MPLS LDP Local Label Allocation Filtering Overview, page 2](#)
- [Prefix Lists for MPLS LDP Local Label Allocation Filtering: Benefits and Description, page 4](#)
- [Local Label Allocation Changes Introduced in Cisco IOS Release 12.2\(33\)SRC and LDP Actions, page 4](#)
- [LDP Local Label Filtering and BGP Routes, page 5](#)

## MPLS LDP Local Label Allocation Filtering Overview

LDP allocates a local label for every route learned from the Interior Gateway Protocol (IGP). In the absence of inbound and outbound label filtering, these local labels are advertised to and learned by all peers.

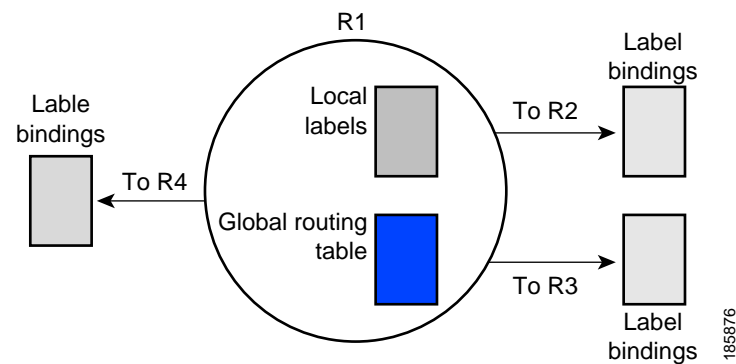
In most Layer 3 Virtual Private Network (VPN) configurations only the label switched paths (LSPs) created to reach the /32 host routes or Border Gateway Protocol (BGP) next hops between the provider edge (PE) routers carry traffic and are relevant to the Layer 3 VPNs. LSPs between the PE routers that are not members of a VPN use more memory and create additional processing in LDP across the core.

With the load increases in the service provider domain in the last decade (1997–2007), scalability has become more important in the service provider networks. Controlling the local label allocation could off-load LDP processing of non-VPN LSPs in the service provider network core devices.

The MPLS LDP—Local Label Allocation Filtering feature introduces the **mpls ldp label** and **allocate** commands that allow you to configure LDP to selectively allocate local labels for a subset of the prefixes learned from the IGP. You can select that LDP allocate local labels for prefixes configured in a prefix list in the global table or for host routes in the global table.

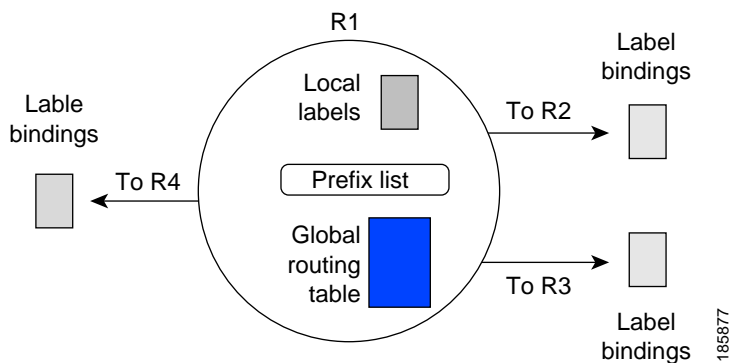
Local label allocation filtering reduces the number of local labels allocated and therefore the number of messages exchanged with peers. This improves LDP scalability and convergence. [Figure 1](#) and [Figure 2](#) show how controlling local label allocation can reduce local label space size and greatly reduce the number of advertisements to peers. [Figure 1](#) shows default LDP label allocation behavior. LDP allocates a local label for every route and advertises a label binding for every route learned from the IGP.

**Figure 1** Default LDP Local Label Allocation Behavior



[Figure 2](#) shows LDP behavior with local label allocation control configured. The size of the local label space and the number of label binding advertisements are reduced with local label allocation filtering through the use of a prefix list. The decrease in the number of local labels and label binding advertisement messages reduces the amount of memory use and improves convergence time for LDP. The MPLS LDP—Local Label Allocation Filtering feature also allows for more efficient use of the label space.

**Figure 2** LDP Behavior with Local Label Allocation Controls



[Figure 2](#) shows that router R1 learns a number of routes from its IGP neighbors on routers R2, R3, and R4. A prefix list defined on router R1 specifies the prefixes for which LDP allocates a local label.

**Note**

In general, the number of Label Information Base (LIB) entries remains the same regardless of the kind of label filtering. This is because the remote label bindings for the prefixes that are filtered are kept in the LIB. Memory use is reduced because local label filtering decreases the number of local labels allocated and the number of label bindings advertised to and stored by the peers of an LSR.

## Prefix Lists for MPLS LDP Local Label Allocation Filtering: Benefits and Description

The MPLS LDP—Local Label Allocation Filtering feature allows you to configure LDP to allocate local labels for a subset of the learned prefixes. LDP accepts the prefix and allocates a local label if the prefix is permitted by a prefix list. If the prefix list is not defined, LDP accepts all prefixes and allocates local labels based on its default mode of operation.

The benefits of using prefix lists for LDP local label allocation filtering are as follows:

- Prefix lists provide more flexibility for specifying a subset of prefixes and masks.
- Prefix lists use a tree-based matching technique. This technique is more efficient than evaluating prefixes or host routes sequentially.
- Prefix lists are easy to modify.

You configure a prefix list for the MPLS LDP—Local Label Allocation Filtering feature with the **ip prefix-list** command. The format of the command is as follows: **ip prefix-list** {*list-name* / *list-number*} [**seq** *number*] {**deny** *network/length* | **permit** *network/length*} [**ge** *ge-length*] [**le** *le-length*]

## Local Label Allocation Changes Introduced in Cisco IOS Release 12.2(33)SRC and LDP Actions

The MPLS LDP—Local Label Allocation Filtering enhancement modifies the LDP's local label allocation handling. The feature supports local label allocation filtering through the specification of a prefix list or host routes.

With the introduction of this feature, LDP needs to determine whether a prefix filter is already configured to control the local label allocation on the local node. If a prefix list exists, the local label allocation is confined to the list of prefixes permitted by the configured prefix list.

LDP also needs to respond to local label allocation configuration changes and to configuration changes that affect the prefix list that LDP is using. Any of the following configuration changes can trigger LDP actions:

- Creating a local label allocation configuration
- Deleting or changing a local label allocation configuration
- Creating a new prefix list for a local label allocation configuration
- Deleting or changing a prefix list for a local label allocation configuration

LDP responds to local label allocation configuration changes by updating the LIB and the forwarding table in the global routing table. To update the LIB after a local label filter configuration change without a session reset, LDP keeps all remote bindings.



If you create a local label allocation configuration without defining a prefix list, no LDP action is required. The local label allocation configuration has no effect because the prefix list is created and permits all prefixes.

If you create or change a prefix list and prefixes that were previously allowed are rejected, LDP goes through a label withdraw and release procedure before the local labels for these prefixes are deallocated.

If you delete a prefix, LDP goes through the label withdraw and release procedure for the LIB local label. If the associated prefix is one for which no LIB entry should be allocated, LDP bypasses this procedure.

The LDP default behavior is to allocate local labels for all non-BGP prefixes. This default behavior does not change with the introduction of this feature and the **mpls ldp label** and **allocate** commands.

**Note**

The local label allocation filtering has no impact on inbound label filtering because both provide LDP filtering independently. The LDP Inbound Label Binding Filtering feature controls label bindings that a label switch router (LSR) accepts from its peer LSRs through the use of access control lists (ACLs). The MPLS LDP—Local Label Allocation Filtering feature controls the allocation of local labels through the use of prefix lists or host routes.

## LDP Local Label Filtering and BGP Routes

The LDP default behavior is to allocate local labels for all non-BGP prefixes.

LDP does not apply the configured local label filter to redistributed BGP routes in the global table for which BGP allocates local label, but LDP does the advertisements (Inter-AS Option C). LDP neither forwards these entries nor releases the local labels allocated by BGP.

## How to Configure MPLS LDP—Local Label Allocation Filtering

Perform the following tasks to configure the MPLS LDP—Local Label Allocation Filtering feature:

- [Creating a Prefix List for MPLS LDP Local Label Allocation Filtering, page 5](#) (optional)
- [Configuring MPLS LDP Local Label Allocation Filtering, page 7](#) (required)
- [Verifying MPLS LDP—Local Label Allocation Filtering Configuration, page 9](#) (optional)

## Creating a Prefix List for MPLS LDP Local Label Allocation Filtering

Perform the following task to create a prefix list for LDP local label allocation filtering. A prefix list allows LDP to selectively allocate local labels for a subset of the routes learned from the IGP. The decrease in the number of local labels in the LDP LIB and the number of label mapping advertisements reduces the amount of memory use and improves convergence time for LDP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** {list-name | list-number} [seq number] {deny network/length | permit network/length} [ge ge-length] [le le-length]

## 4. end

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>ip prefix-list</b> { <i>list-name</i>   <i>list-number</i> } [ <i>seq number</i> ] { <b>deny</b> <i>network/length</i>   <b>permit</b> <i>network/length</i> } [ <b>ge</b> <i>ge-length</i> ] [ <b>le</b> <i>le-length</i> ]<br><br><b>Example:</b><br>Router(config)# ip prefix-list list1 permit 192.168.0.0/16 le 20 | Creates a prefix list or adds a prefix-list entry. <ul style="list-style-type: none"> <li>The <i>list-name</i> argument configures a name to identify the prefix list.</li> <li>The <i>list-number</i> argument configures a number to identify the prefix list.</li> <li>The <b>seq number</b> keyword and argument apply a sequence number to a prefix-list entry. The range of sequence numbers that can be entered is from 1 to 4294967294. If a sequence number is not entered when this command is configured, a default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.</li> <li>The <b>deny</b> keyword denies access for a matching condition.</li> <li>The <b>permit</b> keyword permits access for a matching condition.</li> <li>The <i>network/length</i> arguments and keyword configure the network address, and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 0 to 32.</li> <li>The <b>ge ge-length</b> keyword and argument specify the lesser value of a range (the “from” portion of the range description) by applying the <i>ge-length</i> argument to the range specified. The <i>ge-length</i> argument represents the minimum prefix length to be matched. The <b>ge</b> keyword represents the greater than or equal to operator.</li> <li>The <b>le le-length</b> keyword and argument specify the greater value of a range (the “to” portion of the range description) by applying the <i>le-length</i> argument to the range specified. The <i>le-length</i> argument represents the maximum prefix length to be matched. The <b>le</b> keyword represents the less than or equal to operator.</li> </ul> |

|        | Command or Action                                   | Purpose                        |
|--------|-----------------------------------------------------|--------------------------------|
| Step 4 | <code>end</code>                                    | Exits to privileged EXEC mode. |
|        | <b>Example:</b><br><code>Router(config)# end</code> |                                |

## Configuring MPLS LDP Local Label Allocation Filtering

Perform the following task to configure LDP local allocation filtering. Configuring filtering policies for selective local label binding assignments by LDP improves LDP scalability and convergence. You can configure either a prefix list or host routes as a filter for local label allocation.



### Note

The **host-routes** keyword for the **allocate** command makes it convenient for you to specify a commonly used set of prefixes.

## Restrictions

A maximum of one local label allocation filter is supported for the global table.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ldp label**
4. **allocate global prefix-list** {*list-name* | *list-number*}
5. **allocate global host-routes**
6. **no allocate global** {**prefix-list** {*list-name* | *list-number*} | **host -routes**}
7. **no mpls ldp label**
8. **exit**
9. **exit**

## DETAILED STEPS

|        | Command or Action                                          | Purpose                                                                              |
|--------|------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                        | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br><code>Router&gt; enable</code>          | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code>                            | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br><code>Router# configure terminal</code> |                                                                                      |

|               | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <pre>mpls ldp label</pre> <p><b>Example:</b><br/>Router(config)# mpls ldp label</p>                                                                                   | Enters MPLS LDP label configuration mode to specify how MPLS LDP handles local label allocation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 4</b> | <pre>allocate global prefix-list {list-name   list-number}</pre> <p><b>Example:</b><br/>Router(config-ldp-lbl)# allocate global prefix-list list1</p>                 | <p>Configures local label allocation filters for learned routes for MPLS LDP.</p> <ul style="list-style-type: none"> <li>The <b>global</b> keyword specifies the global routing.</li> <li>The <b>prefix-list</b> keyword specifies a prefix list to be used as a filter for MPLS LDP local label allocation.</li> <li>The <i>list-name</i> argument indicates a name that identifies the prefix list.</li> <li>The <i>list-number</i> argument indicates a number that identifies the prefix list.</li> </ul>                                                                                                                                                 |
| <b>Step 5</b> | <pre>allocate global host-routes</pre> <p><b>Example:</b><br/>Router(config-ldp-lbl)# allocate global host-routes</p>                                                 | <p>Configures local label allocation filters for learned routes for MPLS LDP.</p> <ul style="list-style-type: none"> <li>The <b>global</b> keyword specifies the global routing.</li> <li>The <b>host-routes</b> keyword specifies that local label allocation be done for host routes only.</li> </ul>                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 6</b> | <pre>no allocate global {prefix-list {list-name   list-number}   host-routes}</pre> <p><b>Example:</b><br/>Router(config-ldp-lbl)# no allocate global host-routes</p> | <p>Removes the specific MPLS LDP local label allocation filter without resetting the LDP session.</p> <ul style="list-style-type: none"> <li>The <b>global</b> keyword specifies the global routing.</li> <li>The <b>prefix-list</b> keyword specifies a prefix list to be used as a filter for MPLS LDP local label allocation.</li> <li>The <i>list-name</i> argument indicates a name that identifies the prefix list.</li> <li>The <i>list-number</i> argument indicates a number that identifies the prefix list.</li> <li>The <b>host-routes</b> keyword specifies that host routes be used as a filter for MPLS LDP local label allocation.</li> </ul> |
| <b>Step 7</b> | <pre>no mpls ldp label</pre> <p><b>Example:</b><br/>Router(config-ldp-lbl)# no mpls ldp label</p>                                                                     | Removes all local label allocation filters configured under the MPLS LDP label configuration mode and restores LDP default behavior for local label allocation without a session reset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 8</b> | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-ldp-lbl)# exit</p>                                                                                               | Exits from MPLS LDP label configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 9</b> | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                                                                                                       | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Verifying MPLS LDP—Local Label Allocation Filtering Configuration

Perform the following task to verify the MPLS LDP—Local Label Allocation Filtering configuration.

### SUMMARY STEPS

1. **enable**
2. **show mpls ldp bindings detail**
3. **debug mpls ldp bindings filter**
4. **exit**

### DETAILED STEPS

---

**Step 1 enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

**Step 2 show mpls ldp bindings detail**

Use this command to verify that local label allocation filtering is configured as you expect. For example:

```
Router# show mpls ldp bindings detail

Advertisement spec:
  Prefix acl = bar
Local label filtering spec: host routes.

lib entry: 10.1.1.1/32, rev 9
lib entry: 10.10.7.0/24, rev 10
lib entry: 10.10.8.0/24, rev 11
lib entry: 10.10.9.0/24, rev 12
lib entry: 10.41.41.41/32, rev 17
lib entry: 10.50.50.50/32, rev 15
lib entry: 10.60.60.60/32, rev 18
lib entry: 10.70.70.70/32, rev 16
lib entry: 10.80.80.80/32, rev 14
```

The output of this command verifies that host routes are configured as the local label allocation filter for the router.

**Step 3 debug mpls ldp binding filter**

Use this command to verify that local label allocation filtering was configured properly and to display how LDP accepts or withdraw labels. For example:

```
Router# debug mpls ldp binding filter

LDP Local Label Allocation Filtering changes debugging is on
.
.
.
```

**Step 4    exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

---

## Configuration Examples for MPLS LDP—Local Label Allocation Filtering

This section contains the following configuration examples for the MPLS LDP—Local Label Allocation Filtering feature:

- [Creating a Prefix List for MPLS LDP Local Label Allocation Filtering: Examples, page 10](#)
- [Configuring MPLS LDP Local Label Allocation Filtering: Examples, page 11](#)
- [Sample MPLS LDP Local Label Allocation Filtering Configuration: Example, page 11](#)

### Creating a Prefix List for MPLS LDP Local Label Allocation Filtering: Examples

The following examples show how to configure a prefix list for MPLS LDP local label allocation filtering.

In this example, prefix list List1 permits only 192.168.0.0/16 prefixes. LDP accepts 192.168.0.0/16 prefixes, but would not assign a local label for the following prefixes: 192.168.0.0/24 and 192.168.2.0/24. For example:

```
configure terminal
!
ip prefix-list List1 permit 192.168.0.0/16
end
```

In the following example, prefix list List2 permits a range of prefixes from 192.168.0.0/16 to /20 prefixes. LDP would accept 192.168.0.0/16 prefixes, but would not assign local labels for the following prefixes: 192.168.0.0/24 and 192.168.2.0/24.

```
configure terminal
!
ip prefix-list List2 permit 192.168.0.0/16 le 20
end
```

In the following example, prefix list List3 permits a range of prefixes greater than /18. LDP would accept 192.168.17.0/20 and 192.168.2.0/24 prefixes, but would not assign a local label for 192.168.0.0/16.

```
configure terminal
!
ip prefix-list List3 permit 192.168.0.0/16 ge 18
end
```

## Configuring MPLS LDP Local Label Allocation Filtering: Examples

The following examples show how to configure MPLS LDP local label allocation filtering.

This examples shows how to allocate a prefix list to be used as a local label allocation filter:

```
configure terminal
!
ip prefix-list List3 permit 192.168.0.0/16 ge 18
!
mpls ldp label
  allocate global prefix-list List3
  exit
exit
```

Prefix list List3, which permits a range of prefixes greater than /18, is configured as the local label allocation filter for the router. LDP would allow 192.168.17.0/20 and 192.168.2.0/24 prefixes, but would withdraw labels for prefixes not in the allowed range.

In the following example, host routes are configured as the local label allocation filter:

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

LDP allocates local labels for host routes that are in the global routing table.

In the following example, a specific local label allocation filter is removed:

```
configure terminal
!
mpls ldp label
  no allocate global host-routes
  exit
exit
```

In the following example, all local label allocation filters configured in MPLS LDP label configuration mode are removed and the default LDP local label allocation is restored without a session reset:

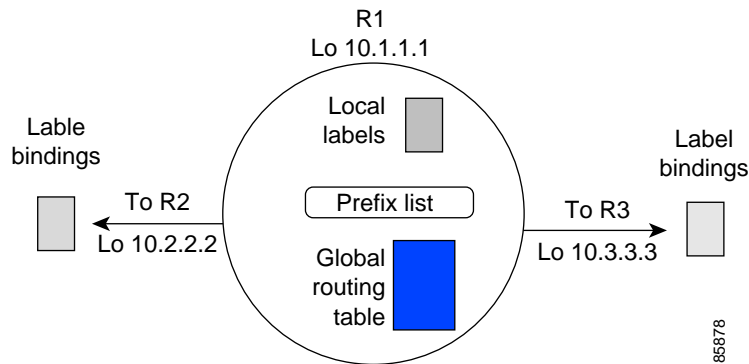
```
configure terminal
!
no mpls ldp label
  exit
exit
```

## Sample MPLS LDP Local Label Allocation Filtering Configuration: Example

Figure 3 is a sample configuration that is used in this section to show how MPLS LDP local label allocation filtering works:

- Routers R1, R2, and R3 have loopback addresses 10.1.1.1, 10.2.2.2, and 10.3.3.3 defined and advertised by the IGP, respectively.
- 10.1.1.1 is the router ID of Router R1, 10.2.2.2 is the router ID of Router R2, and 10.3.3.3 is the router ID of Router R3.
- A prefix list is defined on Router R1 to specify the local labels for which LDP allocates a local label.

Router R1 learns a number of routes from its IGP neighbors on Routers R2 and R3.

**Figure 3 LDP Local Label Allocation Filtering Example**

You can use LDP CLI commands to verify the following:

- Router R1 has allocated a local label for the correct subset of the prefixes.
- Routers R2 and R3 did not receive any remote bindings for the prefixes for which Router R1 did not assign a local label.

## Routing Table on Router R1

You can enter the **show ip route** command to display the current state of the routing table. The following example shows the routing table on Router R1 based on Figure 3:

```
R1# show ip route
```

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

```
Gateway of last resort is not set
```

```
10.0.0.0/32 is subnetted, 1 subnets
C    10.1.1.1 is directly connected, Loopback0
10.2.0.0/32 is subnetted, 1 subnets
O    10.2.2.2 [110/11] via 10.10.7.1, 00:00:36, Ethernet1/0
10.3.0.0/32 is subnetted, 1 subnets
O    10.3.3.3 [110/11] via 10.10.9.1, 00:00:36, Ethernet3/0
10.0.0.0/24 is subnetted, 3 subnets
C    10.10.7.0 is directly connected, Ethernet1/0
O    10.10.8.0 [110/20] via 10.10.9.1, 00:00:36, Ethernet3/0
     [110/20] via 10.10.7.1, 00:00:36, Ethernet1/0
C    10.10.9.0 is directly connected, Ethernet3/0
```

## Local Label Bindings on Router R1, Router R2, and Router R3

You can enter the **show mpls ldp bindings** command on Routers R1, R2, and R3 to display the contents of the LIB on each router. In the following examples, the default LDP allocation behavior is in operation; that is, LDP allocates a local label for every route and advertises a label binding for every route learned from the IGP.



### LIB on Router R

This example shows the contents of the LIB on Router R1 based on the configuration in [Figure 3](#):

```
R1# show mpls ldp bindings

lib entry: 10.1.1.1/32, rev 7
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: 16
    remote binding: lsr: 10.2.2.2:0, label: 17
lib entry: 10.2.2.2/32, rev 13
    local binding:  label: 1000
    remote binding: lsr: 10.3.3.3:0, label: 18
    remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.3.3.3/32, rev 15
    local binding:  label: 1002
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.2.2.2:0, label: 18
lib entry: 10.10.7.0/24, rev 8
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: 17
    remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.8.0/24, rev 11
    local binding:  label: 1001
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.9.0/24, rev 9
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.2.2.2:0, label: 16
```

The local labels assigned to 10.2.2.2 and 10.3.3.3 on Router R1 are advertised to Routers R2 and R3.

### LIB on Router R2

This example shows the contents of the LIB on Router R2 based on the configuration in [Figure 3](#):

```
R2# show mpls ldp bindings

lib entry: 10.1.1.1/32, rev 11
    local binding:  label: 17
    remote binding: lsr: 10.3.3.3:0, label: 16
    remote binding: lsr: 10.1.1.1:0, label: imp-null
lib entry: 10.2.2.2/32, rev 7
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: 18
    remote binding: lsr: 10.1.1.1:0, label: 1000
lib entry: 10.3.3.3/32, rev 15
    local binding:  label: 18
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.1.1.1:0, label: 1002
lib entry: 10.10.7.0/24, rev 8
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: 17
    remote binding: lsr: 10.1.1.1:0, label: imp-null
lib entry: 10.10.8.0/24, rev 9
    local binding:  label: imp-null
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.1.1.1:0, label: 1001
lib entry: 10.10.9.0/24, rev 13
    local binding:  label: 16
    remote binding: lsr: 10.3.3.3:0, label: imp-null
    remote binding: lsr: 10.1.1.1:0, label: imp-null
```

**LIB on Router R3**

This example shows the contents of the LIB on Router R3 based on the configuration in [Figure 3](#):

R3# **show mpls ldp bindings**

```
lib entry: 10.1.1.1/32, rev 13
  local binding: label: 16
  remote binding: lsr: 10.2.2.2:0, label: 17
  remote binding: lsr: 10.1.1.1:0, label: imp-null
lib entry: 10.2.2.2/32, rev 15
  local binding: label: 18
  remote binding: lsr: 10.2.2.2:0, label: imp-null
  remote binding: lsr: 10.1.1.1:0, label: 1000
lib entry: 10.3.3.3/32, rev 7
  local binding: label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: 18
  remote binding: lsr: 10.1.1.1:0, label: 1002
lib entry: 10.10.7.0/24, rev 11
  local binding: label: 17
  remote binding: lsr: 10.2.2.2:0, label: imp-null
  remote binding: lsr: 10.1.1.1:0, label: imp-null
lib entry: 10.10.8.0/24, rev 8
  local binding: label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: imp-null
  remote binding: lsr: 10.1.1.1:0, label: 1001
lib entry: 10.10.9.0/24, rev 9
  local binding: label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: 16
  remote binding: lsr: 10.1.1.1:0, label: imp-null
```

**Local Label Allocation Filtering Configuration on Router R1**

You enter the **mpls ldp label** command to configure a local label allocation filter. The following examples show how to configure a local label allocation filter by host routes only and by a prefix list.

**Local Label Allocation Filter—Host Routes Only Configuration**

This example shows the selection of host routes as the only filter.

The following local label allocation filtering is defined on Router R1 under MPLS LDP label configuration mode:

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

**Local Label Allocation Filter—Prefix List Configuration**

The following example shows how to configure a local label allocation filter that allows or denies prefixes based on a prefix list:

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

ListA is a prefix list defined as:

```
configure terminal
!
ip prefix-list ListA permit 0.0.0.0/32 ge 32
```

## Local Label Allocation Filtering Changes Label Bindings on Router R1, Router R2, and Router R3

After configuring a local label allocation filter on Router R1, you can enter the **show mpls ldp bindings** command again to see the changes in the local label bindings in the LIB on each router. Changes to the output in the LIB entries are highlighted in bold text.

This sample prefix list is used for the examples in this section:

```
ip prefix-list ListA permit 0.0.0.0/32 ge 32
```

### LIB on Router R1 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter changes the contents of the LIB on Router R1:

R1# **show mpls ldp bindings**

```
lib entry: 10.1.1.1/32, rev 7
  local binding: label: imp-null
  remote binding: lsr: 10.3.3.3:0, label: 16
  remote binding: lsr: 10.2.2.2:0, label: 17
lib entry: 10.2.2.2/32, rev 13
  local binding: label: 1000
  remote binding: lsr: 10.3.3.3:0, label: 18
  remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.3.3.3/32, rev 15
  local binding: label: 1002
  remote binding: lsr: 10.3.3.3:0, label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: 18
lib entry: 10.10.7.0/24, rev 8
  no local binding
  remote binding: lsr: 10.3.3.3:0, label: 17
  remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.8.0/24, rev 11
  no local binding
  remote binding: lsr: 10.3.3.3:0, label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.9.0/24, rev 9
  no local binding
  remote binding: lsr: 10.3.3.3:0, label: imp-null
  remote binding: lsr: 10.2.2.2:0, label: 16
```

Local label bindings for all but 10.2.2.2 and 10.3.3.3 on Router R1 are advertised as withdrawn.

### LIB on Router R2 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter on Router R1 changes the contents of the LIB on Router R2:

R2# **show mpls ldp bindings**

```
lib entry: 10.1.1.1/32, rev 11
  local binding: label: 17
  remote binding: lsr: 10.3.3.3:0, label: 16
lib entry: 10.2.2.2/32, rev 7
```

```

        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1000
lib entry: 10.3.3.3/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.3.3.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1002
lib entry: 10.10.7.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: 17
lib entry: 10.10.8.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.3.3.3:0, label: imp-null
lib entry: 10.10.9.0/24, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.3.3.3:0, label: imp-null

```

The 10.10.7.0/24, 10.10.8.0/24, and 10.10.9.0/24 prefixes are no longer assigned local labels. Therefore, Router R1 sends no label advertisement for these prefixes.

### LIB on Router R3 After Local Label Allocation Filtering

This example shows how the configuration of a local label allocation prefix-list filter on Router R1 changes the contents of the LIB on Router R3:

R3# **show mpls ldp bindings**

```

lib entry: 10.1.1.1/32, rev 13
        local binding:  label: 16
        remote binding: lsr: 10.2.2.2:0, label: 17
        remote binding: lsr: 10.1.1.1:0, label: imp-null
lib entry: 10.2.2.2/32, rev 15
        local binding:  label: 18
        remote binding: lsr: 10.2.2.2:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 1000
lib entry: 10.3.3.3/32, rev 7
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 18
        remote binding: lsr: 10.1.1.1:0, label: 1002
lib entry: 10.10.7.0/24, rev 11
        local binding:  label: 17
        remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.8.0/24, rev 8
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: imp-null
lib entry: 10.10.9.0/24, rev 9
        local binding:  label: imp-null
        remote binding: lsr: 10.2.2.2:0, label: 16

```

The 10.10.7.0/24, 10.10.8.0/24, and 10.10.9.0/24 prefixes are no longer assigned local labels. Again, Router R1 sends no label advertisement for these prefixes.

## Command to Display the Local Label Allocation Filter

You can enter the **show mpls ldp detail** command to display the filter used for local label allocation. For example:

Router# **show mpls ldp bindings detail**

```

Advertisement spec:
  Prefix acl = List1
Local label filtering spec: host routes. ! <--- Local local label filtering spec

```

```
lib entry: 10.1.1.1/32, rev 9
lib entry: 10.10.7.0/24, rev 10
lib entry: 10.10.8.0/24, rev 11
lib entry: 10.10.9.0/24, rev 12
lib entry: 10.41.41.41/32, rev 17
lib entry: 10.50.50.50/32, rev 15
lib entry: 10.60.60.60/32, rev 18
lib entry: 10.70.70.70/32, rev 16
lib entry: 10.80.80.80/32, rev 14
```

## Additional References

The following sections provide references related to the MPLS LDP—Local Label Allocation Filtering feature.

## Related Documents

| Related Topic                                                        | Document Title                                                            |
|----------------------------------------------------------------------|---------------------------------------------------------------------------|
| Configuration tasks for MPLS LDP                                     | <a href="#">MPLS Label Distribution Protocol Overview</a>                 |
| MPLS LDP commands                                                    | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |
| Configuration tasks for inbound label binding filtering for MPLS LDP | <a href="#">MPLS LDP Inbound Label Binding Filtering</a>                  |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| RFC 3037 | <a href="#"><i>LDP Applicability</i></a>                                                                                              |
| RFC 3815 | <a href="#"><i>Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)</i></a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **allocate**
- **debug mpls ldp bindings**
- **mpls ldp label**
- **show mpls ldp bindings**

# Feature Information for MPLS LDP—Local Label Allocation Filtering

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS LDP—Local Label Allocation Filtering

| Feature Name                              | Releases                  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS LDP—Local Label Allocation Filtering | 12.2(33)SRC<br>12.2(33)SB | <p>This feature introduces command-line interface (CLI) commands to modify the way in which Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) handles local label allocation. This MPLS LDP feature enhancement enables the configuration of filtering policies for selective local label binding assignments by LDP to improve LDP scalability and convergence. This document contains information about and instructions on how to configure the MPLS LDP—Local Label Allocation Filtering feature.</p> <p>In 12.2(33)SRC, the feature was introduced on a Cisco IOS 12.2SR release.</p> <p>In 12.2(33)SB, the feature was integrated into a Cisco IOS 12.2SB release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS LDP Local Label Allocation Filtering Overview, page 2</a></li> <li>• <a href="#">Prefix Lists for MPLS LDP Local Label Allocation Filtering: Benefits and Description, page 4</a></li> <li>• <a href="#">Local Label Allocation Changes Introduced in Cisco IOS Release 12.2(33)SRC and LDP Actions, page 4</a></li> <li>• <a href="#">LDP Local Label Filtering and BGP Routes, page 5</a></li> <li>• <a href="#">Creating a Prefix List for MPLS LDP Local Label Allocation Filtering, page 5</a></li> </ul> |

**Table 1**      *Feature Information for MPLS LDP—Local Label Allocation Filtering (continued)*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <ul style="list-style-type: none"> <li>• <a href="#">Configuring MPLS LDP Local Label Allocation Filtering, page 7</a></li> <li>• <a href="#">Verifying MPLS LDP—Local Label Allocation Filtering Configuration, page 9</a></li> </ul> <p>The following commands were introduced or modified:<br/> <b>allocate</b>, <b>debug mpls ldp bindings</b>, <b>mpls ldp label</b>, <b>show mpls ldp bindings</b>.</p> |



# Glossary

**BGP**—Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. It is defined by RFC 1163.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers do not have routes to associated Virtual Private Networks (VPNs) in their routing tables.

**FEC**—Forwarding Equivalency Class. A set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within a single autonomous system. Examples of common Internet IGP protocols include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Routing Information protocol (RIP).

**label**—A short fixed-length label that tells switching nodes how to forward data (packets or cells).

**LDP**—Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

**LIB**—Label Information Base. A database used by a label switch router (LSR) to store labels learned from other LSRs, and labels assigned by the local LSR.

**LSP**—label switched path. A sequence of hops in which a packet travels from one router to another router by means of label switching mechanisms. A label switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

**LSR**—label switch router. A device that forwards Multiprotocol Label Switching (MPLS) packets based on the value of a fixed-length label encapsulated in each packet.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

**PE router**—provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All Virtual Private Network (VPN) processing occurs in the PE router.

**VPN**—Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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

© 2008 Cisco Systems, Inc. All rights reserved.



## **MPLS Traffic Engineering: Path Calculation and Setup**





# MPLS Traffic Engineering—LSP Attributes

---

**First Published: August 26, 2003**

**Last Updated: February 18, 2009**

This document describes how to configure label switched path (LSP) attributes for path options associated with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

The MPLS Traffic Engineering—LSP Attributes feature is an extension to MPLS TE that provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features provide flexibility in the configuration of LSP attributes for MPLS TE tunnel path options. Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a path option for bandwidth override.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS Traffic Engineering—LSP Attributes](#)” section on page 42.

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—LSP Attributes](#), page 2
- [Restrictions for MPLS Traffic Engineering—LSP Attributes](#), page 2
- [Information About MPLS Traffic Engineering—LSP Attributes](#), page 2
- [How to Configure MPLS Traffic Engineering—LSP Attributes](#), page 6
- [Configuration Examples for MPLS Traffic Engineering—LSP Attributes](#), page 34
- [Additional References](#), page 39



---

**Americas Headquarters:**

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

© 2003—2009 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 40](#)
- [Feature Information for MPLS Traffic Engineering—LSP Attributes, page 42](#)
- [Glossary, page 44](#)

## Prerequisites for MPLS Traffic Engineering—LSP Attributes

The MPLS Traffic Engineering—LSP Attributes feature requires that you configure an MPLS TE tunnel before you configure either an LSP Attribute List or a Path Option for Bandwidth Override feature.

## Restrictions for MPLS Traffic Engineering—LSP Attributes

Reoptimization between path options with different bandwidth pool types (subpool versus global pool) and different priorities is not supported. Specifically,

- With the Path Option for Bandwidth Override feature, you need to configure bandwidth for path options with the same bandwidth pool as configured for the tunnel.
- With the LSP Attribute List feature, you need to configure both a bandwidth pool and priority for path options that are consistent with the bandwidth pool and priority configured on the tunnel or in other path options used by the tunnel.

## Information About MPLS Traffic Engineering—LSP Attributes

To configure the MPLS Traffic Engineering—LSP Attributes feature, you need the following information:

- [MPLS Traffic Engineering—LSP Attributes Benefits, page 2](#)
- [Traffic Engineering Bandwidth and Bandwidth Pools, page 3](#)
- [LSP Attribute Lists Usage and Management, page 3](#)
- [Autobandwidth and Path Option for Bandwidth Override, page 4](#)
- [Path Option Selection for MPLS TE Tunnel LSPs, page 5](#)

## MPLS Traffic Engineering—LSP Attributes Benefits

The MPLS Traffic Engineering—LSP Attributes provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features have the following benefits:

- The LSP Attributes List feature provides the ability to configure values for several LSP-specific path options for TE tunnels.
- One or more TE tunnels can specify specific path options by referencing an LSP attribute list.

- LSP attribute lists make the MPLS TE user interface more flexible, easier to use, and easier to extend and maintain.
- The Path Option for Bandwidth Override feature provides a single command that allows a TE tunnel to fall back temporarily to path options that can reduce bandwidth constraints.

## Traffic Engineering Bandwidth and Bandwidth Pools

MPLS traffic engineering allows constraint-based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Regular TE tunnel bandwidth is called the global pool. Subpool bandwidth is a portion of the global pool. Subpool bandwidth is not reserved from the global pool if it is not in use. Therefore, subpool tunnels require a higher priority than nonsubpool tunnels.

You can configure the LSP Attributes bandwidth path option to use either global pool (default) or subpool bandwidth. The bandwidth value for the path option may be any valid value and the pool does not have to be the same as that configured on the tunnel.



### Note

When you configure bandwidth for path options with the **bandwidth [sub-pool | global] kbps** command, use either all subpool bandwidths or all global-pool bandwidths.

You can configure bandwidth on both dynamic and explicit path options using either the LSP Attribute List feature or the Path Option for Bandwidth Override feature. The commands that enable these features are exclusive of each other. If bandwidth is the only LSP attribute that you need to set on the path option, then use the command to enable the Path Option for Bandwidth Override feature. This is the simplest way to configure multiple path options with decreasing bandwidth constraints. Once the **bandwidth** keyword is entered on the **tunnel mpls traffic-eng path-option** command in interface configuration mode, you cannot configure an LSP attribute list for that path option.

## LSP Attribute Lists Usage and Management

This section contains the following topics about LSP attribute lists usage and management:

- [Tunnel Attributes and LSP Attributes, page 3](#)
- [LSP Attributes and the LSP Attribute List, page 4](#)
- [LSP Attribute Lists Management, page 4](#)

## Tunnel Attributes and LSP Attributes

Cisco IOS tunneling interfaces have many parameters associated with MPLS TE. Typically, you configure these parameters with **tunnel mpls traffic-eng** commands in interface configuration mode. Many of these commands determine tunnel-specific properties, such as the load-sharing factor for the tunnel. These commands configure parameters that are unrelated to the particular LSP in use by the tunnel. However, some of the tunneling parameters apply to the LSP that the tunnel uses. You can configure the LSP-specific properties using an LSP attribute list.

## LSP Attributes and the LSP Attribute List

An LSP attribute list can contain values for each LSP-specific parameter that is configurable for a TE tunnel. You configure an LSP attribute list with the **mpls traffic-eng lsp attributes** *string* command, where *string* identifies the attribute list. The LSP attributes that you can specify include the following:

- Attribute flags for links that make up the LSP (**affinity** command)
- Automatic bandwidth configuration (**auto-bw** command)
- LSP bandwidth—global pool or subpool (**bandwidth** command)
- Disable reoptimization of the LSP (**lockdown** command)
- LSP priority (**priority** command)
- Protection failure (**protection** command)
- Record the route used by the LSP (**record-route** command)

## LSP Attribute Lists Management

The MPLS Traffic Engineering—LSP Attributes feature also provides commands that help you manage LSP attribute lists. You can do the following:

- Relist all attribute list entries (**list** command)
- Remove a specific attribute from the list (**no attribute** command)

The **exit** command exits from the LSP attributes configuration submode and returns you to global configuration mode.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

## Autobandwidth and Path Option for Bandwidth Override

If Traffic Engineering automatic bandwidth (autobandwidth) adjustment is configured for a tunnel, traffic engineering automatically adjusts the bandwidth allocation for the traffic engineering tunnel based on its measured usage of the bandwidth of the tunnel.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically adjusts the allocated bandwidth for the tunnel to be the largest sample for the tunnel since the last adjustment. The default reoptimization setting in the MPLS AutoBandwidth feature is every 24 hours

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

For more information on automatic bandwidth adjustment for TE tunnels, see the *MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels* feature documentation.

The Path Option for Bandwidth Override feature allows you to override the bandwidth configured on a TE tunnel. This feature also overrides bandwidth configured or recalculated by automatic bandwidth adjustment if the path option in effect has bandwidth override enabled.



## Path Option Selection for MPLS TE Tunnel LSPs

This section contains the following topics about path option selection for MPLS TE Tunnel LSPs:

- [Constraint-Based Routing and Path Option Selection, page 5](#)
- [Tunnel Reoptimization and Path Option Selection, page 5](#)
- [Path Option Selection with Bandwidth Override, page 6](#)

### Constraint-Based Routing and Path Option Selection

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone by using the Resource Reservation Protocol (RSVP). The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth. Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint-based routing).

Without the Path Option for Bandwidth Override feature, a TE tunnel establishes an LSP based on dynamic or explicit path options in order of preference. However, the bandwidth and other attributes configured on the TE tunnel allow the setup of an LSP only if LSP path options satisfy the constraints. If a path cannot be found that satisfies the configured path options, then the tunnel is not set up.

The Path Option for Bandwidth Override feature provides a fallback path option that allows overriding the bandwidth configured on the TE tunnel interface. For example, you can configure a path option that sets the bandwidth to zero (0) effectively removing the bandwidth constraint imposed by the constraint-based routing calculation.

### Tunnel Reoptimization and Path Option Selection

Reoptimization occurs when a device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP. If the signaling is successful, the device replaces the older LSP with the new, better LSP.

Reoptimization can be triggered by a timer, the issuance of an **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of a tunnel. The MPLS AutoBandwidth feature, for example, uses a timer to set the frequency of reoptimization based on the bandwidth path option attribute. The Path Option for Bandwidth Override feature allows for the switching between bandwidth configured on the TE tunnel interface and bandwidth configured on a specific path option. This increases the success of signaling an LSP for the TE tunnel.

With bandwidth override configured on a path option, the traffic engineering software attempts to reoptimize the bandwidth every 30 seconds to reestablish the bandwidth configured on the tunnel (see the [“Configuring a Path Option for Bandwidth Override” section on page 26](#)).

You can disable reoptimization of an LSP with the **lockdown** command in an LSP attribute list. You can apply the LSP attribute list containing the **lockdown** command to a path option with the **tunnel mpls traffic-eng path-option** command.



#### Note

When you configure bandwidth for path options with the **bandwidth [sub-pool | global] kpbs** command, use either all subpool bandwidths or all global-pool bandwidths. Do not mix subpool and nonsubpool bandwidths, otherwise the path option does not reoptimize later.

## Path Option Selection with Bandwidth Override

The Path Option for Bandwidth Override feature allows you to configure bandwidth parameters on a specific path option with the **bandwidth** keyword on the **tunnel mpls traffic-eng path-option** command. When an LSP is signaled using a path option with a configured bandwidth, the bandwidth associated with the path option is signaled instead of the bandwidth configured directly on the tunnel.

This feature provides you with the ability to configure multiple path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

The following configuration shows three **tunnel mpls traffic-eng path-option** commands:

```
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name path1
tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
```

The device selects a path option for an LSP in order of preference, as follows:

- The device attempts to signal an LSP using path options starting with path option 1.  
The device attempts to signal an LSP with the 1000 kbps bandwidth configured on the tunnel interface because path-option 1 has no bandwidth configured.
- If 1000 kbps bandwidth is not available over the network, the device attempts to establish an LSP using path-option 2.  
Path option 2 has a bandwidth of 500 kbps configured. This reduces the bandwidth constraint from the original 1000 kbps configured on the tunnel interface.
- If 500 kbps is not available, the device attempts to establish an LSP using path-option 3.  
Path-option 3 is configured as dynamic and has bandwidth 0. The device establishes the LSP if an IP path exists to the destination and all other tunnel constraints are met.

## How to Configure MPLS Traffic Engineering—LSP Attributes

This section contains the following processes for configuring the MPLS Traffic Engineering—LSP Attributes feature:

- [Configuring MPLS Traffic Engineering LSP Attribute Lists, page 6](#)
- [Configuring a Path Option for Bandwidth Override, page 26](#)

## Configuring MPLS Traffic Engineering LSP Attribute Lists

Perform the following tasks to configure and verify MPLS traffic engineering LSP attributes lists:

- [Configuring an LSP Attribute List, page 7](#) (required)
- [Adding Attributes to an LSP Attribute List, page 9](#) (optional)
- [Removing an Attribute from an LSP Attribute List, page 11](#) (optional)
- [Modifying an Attribute in an LSP Attribute List, page 12](#) (optional)
- [Deleting an LSP Attribute List, page 14](#) (optional)
- [Verifying Attributes Within an LSP Attribute List, page 15](#) (optional)
- [Verifying All LSP Attribute Lists, page 16](#) (optional)

- [Associating an LSP Attribute List with a Path Option for an MPLS TE Tunnel, page 17](#) (required)
- [Modifying a Path Option to Use a Different LSP Attribute List, page 21](#) (optional)
- [Removing a Path Option for an LSP for an MPLS TE Tunnel, page 23](#) (optional)
- [Verifying that LSP Is Signaled Using the Correct Attributes, page 25](#) (optional)

## Configuring an LSP Attribute List

Perform this task to configure a label switched path (LSP) attribute list with the desired attributes to be applied on a path option. Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. The LSP attribute list provides a user interface that is flexible, easy to use, and easy to extend and maintain for the configuration of MPLS TE tunnel path options.

LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask** *value*]
5. **auto-bw** [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]
6. **bandwidth** [**sub-pool** | **global**] *kbps*
7. **list**
8. **lockdown**
9. **priority** *setup-priority* [*hold-priority*]
10. **protection fast-reroute**
11. **record-route**
12. **no** *sub-command*
13. **exit**
14. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |

|        | Command or Action                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>mpls traffic-eng lsp attributes</b> <i>string</i><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng lsp attributes 1                                                             | Configures an LSP attribute list and enters LSP Attributes configuration mode. <ul style="list-style-type: none"> <li>The <i>string</i> argument identifies a specific LSP attribute list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>affinity</b> <i>value</i> [ <b>mask</b> <i>value</i> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# affinity 0 mask 0                                                               | (Optional) Specifies attribute flags for links comprising an LSP. <ul style="list-style-type: none"> <li>The <i>value</i> argument is a value required for links that make up an LSP. Values of the bits are either 0 or 1.</li> <li>The <b>mask</b> <i>value</i> keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> <li>If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.</li> <li>If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match.</li> </ul> </li> </ul>                                                                                                                                                                             |
| Step 5 | <b>auto-bw</b> [ <b>frequency</b> <i>secs</i> ] [ <b>max-bw</b> <i>kbps</i> ] [ <b>min-bw</b> <i>kbps</i> ] [ <b>collect-bw</b> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# auto-bw | (Optional) Specifies automatic bandwidth configuration. <ul style="list-style-type: none"> <li>The <b>frequency</b> <i>secs</i> keyword argument combination specifies the interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds.</li> <li>The <b>max-bw</b> <i>kbps</i> keyword argument combination specifies the maximum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295.</li> <li>The <b>min-bw</b> <i>kbps</i> keyword argument combination specifies the minimum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295.</li> <li>The <b>collect-bw</b> keyword collects output rate information for the path option, but does not adjust the bandwidth of the path option.</li> </ul> |
| Step 6 | <b>bandwidth</b> [ <b>sub-pool</b>   <b>global</b> ] <i>kbps</i><br><br><b>Example:</b><br>Router(config-lsp-attr)# bandwidth 5000                                                           | (Optional) Specifies LSP bandwidth. <ul style="list-style-type: none"> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> </ul>                                                                                                                                                                                                                                                                                                             |
| Step 7 | <b>list</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# list                                                                                                                          | (Optional) Displays the contents of the LSP attribute list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|         | Command or Action                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <code>lockdown</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# lockdown                                    | (Optional) Disables reoptimization of the LSP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 9  | <code>priority setup-priority [hold-priority]</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# priority 1 1 | (Optional) Specifies the LSP priority. <ul style="list-style-type: none"> <li>The <i>setup-priority</i> argument is used when signaling an LSP to determine which existing LSPs can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.</li> <li>The <i>hold-priority</i> argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.</li> </ul> |
| Step 10 | <code>protection fast-reroute</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# protection fast-reroute      | (Optional) Enables failure protection on the LSP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 11 | <code>record-route</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# record-route                            | (Optional) Records the route used by the LSP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 12 | <code>no sub-command</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# no record-route                       | (Optional) Removes a specific attribute from the LSP attributes list. <ul style="list-style-type: none"> <li>The <i>sub-command</i> argument names the LSP attribute to remove from the attributes list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 13 | <code>exit</code><br><br><b>Example:</b><br>Router(config-lsp-attr)# exit                                            | (Optional) Exits from LSP Attributes configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 14 | <code>end</code><br><br><b>Example:</b><br>Router(config)# end                                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Adding Attributes to an LSP Attribute List

Perform this task to add attributes to an LSP attribute list. The LSP attribute list provides a user interface that is flexible, easy to use, and that can be extended or changed at any time to meet the requirements of your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attributes list and to add or change the required path option attribute.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask** *value*]
5. **bandwidth** [**sub-pool** | **global**] *kbps*
6. **priority** *setup-priority* [*hold-priority*]
7. **list**
8. **exit**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>mpls traffic-eng lsp attributes</b> <i>string</i><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng lsp attributes 1 | Configures an LSP attribute list and enters LSP Attributes configuration mode.<br><ul style="list-style-type: none"><li>The <i>string</i> argument identifies a specific LSP attribute list.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 4 | <b>affinity</b> <i>value</i> [ <b>mask</b> <i>value</i> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# affinity 0 mask 0   | (Optional) Specifies attribute flags for links comprising an LSP.<br><ul style="list-style-type: none"><li>The <i>value</i> argument is a value required for links that make up an LSP. Values of the bits are either 0 or 1.</li><li>The <b>mask</b> <i>value</i> keyword argument combination indicates which attribute values should be checked.<ul style="list-style-type: none"><li>If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.</li><li>If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match.</li></ul></li></ul> |

|        | Command or Action                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>bandwidth</b> [ <b>sub-pool</b>   <b>global</b> ] <i>kbps</i><br><br><b>Example:</b><br>Router(config-lsp-attr)# bandwidth 1000 | Specifies an LSP bandwidth. <ul style="list-style-type: none"> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> </ul>                                                                                                             |
| Step 6 | <b>priority</b> <i>setup-priority</i> [ <i>hold-priority</i> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# priority 2 2     | Specifies the LSP priority. <ul style="list-style-type: none"> <li>The <i>setup-priority</i> argument is used when signaling an LSP to determine which existing LSPs can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.</li> <li>The <i>hold-priority</i> argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.</li> </ul> |
| Step 7 | <b>list</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# list                                                                | (Optional) Displays the contents of the LSP attribute list. <ul style="list-style-type: none"> <li>Use the <b>list</b> command to display the path option attributes added to the attribute list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# exit                                                                | (Optional) Exits LSP Attributes configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                           | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Removing an Attribute from an LSP Attribute List

Perform this task to remove an attribute from an LSP attribute list. The LSP attributes list provides a means to easily remove a path option attribute that is no longer required for your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attribute list and for the **no sub-command** command, which is used to remove the specific attribute from the list. Replace the *sub-command* argument with the command that you want to remove from the list.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **mpls traffic-eng lsp attributes** *string*
4. **no** *sub-command*
5. **list**
6. **exit**
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                   | Enters global configuration mode.                                                                                                                                                                                         |
| Step 3 | <b>mpls traffic-eng lsp attributes</b> <i>string</i><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng lsp attributes 1 | Configures an LSP attribute list and enters LSP Attributes configuration mode.<br><ul style="list-style-type: none"> <li>The <i>string</i> argument identifies a specific LSP attribute list.</li> </ul>                  |
| Step 4 | <b>no</b> <i>sub-command</i><br><br><b>Example:</b><br>Router(config-lsp-attr)# no priority                                      | Removes a specific attribute from the LSP attribute list.<br><ul style="list-style-type: none"> <li>The <i>sub-command</i> argument names the LSP attribute to remove from the attributes list.</li> </ul>                |
| Step 5 | <b>list</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# list                                                              | (Optional) Displays the contents of the LSP attribute list.<br><ul style="list-style-type: none"> <li>Use the <b>list</b> command to verify that the path option attribute is removed from the attribute list.</li> </ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# exit                                                              | (Optional) Exits LSP Attributes configuration mode.                                                                                                                                                                       |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                         | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                 |

## Modifying an Attribute in an LSP Attribute List

Perform this task to modify an attribute in an LSP attribute list. The LSP attribute list provides a flexible user interface that can be extended or modified any time to meet the requirements of your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attributes list and to modify the required path option attribute.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask** *value*]
5. **list**
6. **affinity** *value* [**mask** *value*]
7. **list**
8. **exit**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>mpls traffic-eng lsp attributes</b> <i>string</i><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng lsp attributes 1 | Configures an LSP attribute list and enters LSP Attributes configuration mode. <ul style="list-style-type: none"> <li>The <i>string</i> argument identifies a specific LSP attribute list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>affinity</b> <i>value</i> [ <b>mask</b> <i>value</i> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# affinity 1 mask 1   | Specifies attribute flags for links comprising an LSP. <ul style="list-style-type: none"> <li>The <i>value</i> argument is a value required for links comprising an LSP. Values of bits are either 0 or 1.</li> <li>The <b>mask</b> <i>value</i> keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> <li>If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.</li> <li>If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.</li> </ul> </li> </ul> |
| Step 5 | <b>list</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# list                                                              | (Optional) Displays the contents of the LSP attribute list. <ul style="list-style-type: none"> <li>Use the <b>list</b> command to display the path option attributes configured in the attribute list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                          |

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>affinity</b> <i>value</i> [ <b>mask</b> <i>value</i> ]<br><br><b>Example:</b><br>Router(config-lsp-attr)# affinity 0 mask 0 | Specifies attribute flags for links comprising an LSP. <ul style="list-style-type: none"> <li>The <i>value</i> argument is a value required for links comprising an LSP. Values of bits are either 0 or 1.</li> <li>The <b>mask</b> <i>value</i> keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> <li>If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.</li> <li>If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.</li> </ul> </li> </ul> |
| Step 7 | <b>list</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# list                                                            | (Optional) Displays the contents of the LSP attribute list. <ul style="list-style-type: none"> <li>Use the <b>list</b> command to verify that the path option attributes is modified in the attribute list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-lsp-attr)# exit                                                            | (Optional) Exits LSP Attributes configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Deleting an LSP Attribute List

Perform this task to delete an LSP attribute list. You would perform this task when you no longer require the LSP attribute path options specified in the LSP attribute list for an MPLS TE tunnel.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no mpls traffic-eng lsp attributes** *string*
4. **end**
5. **show mpls traffic-eng lsp attributes** [*string*]

## DETAILED STEPS

|        | Command or Action                                                                                                                      | Purpose                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                         | Enters global configuration mode.                                                                                                                                                                                                                      |
| Step 3 | <b>no mpls traffic-eng lsp attributes <i>string</i></b><br><br><b>Example:</b><br>Router(config)# no mpls traffic-eng lsp attributes 1 | Removes a specified LSP attribute list from the device configuration. <ul style="list-style-type: none"> <li>The <i>string</i> argument identifies the specific LSP attribute list to remove.</li> </ul>                                               |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                               | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                              |
| Step 5 | <b>show mpls traffic-eng lsp attributes [<i>string</i>]</b><br><br><b>Example:</b><br>Router# show mpls traffic-eng lsp attributes     | (Optional) Displays information about configured LSP attribute lists. <ul style="list-style-type: none"> <li>Use the <b>show mpls traffic-eng lsp attributes</b> command to verify that the LSP attribute list was deleted from the router.</li> </ul> |

## Verifying Attributes Within an LSP Attribute List

Perform this task to verify attributes within an LSP attribute list.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes *string* list**
4. **exit**
5. **end**

## DETAILED STEPS

|        |                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br>Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:<br><br>Router> <b>enable</b><br>Router# |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Step 2**    **configure terminal**

Use this command to enter global configuration mode. For example:

```
Router# configure terminal
Router(config)#
```

**Step 3**    **mpls traffic-eng lsp attributes *string* list**

Use this command to enter LSP Attributes configuration mode for a specific LSP attribute list and to verify that the contents of the attributes list are as expected. For example:

```
Router(config)# mpls traffic-eng lsp attributes 1 list

LIST 1
  bandwidth 1000
  priority 1 1
```

**Step 4**    **exit**

Use this command to exit LSP Attributes configuration mode. For example:

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

**Step 5**    **end**

Use this command to exit to privileged EXEC mode. For example:

```
Router(config)# exit
Router#
```

---

## Verifying All LSP Attribute Lists

Perform this task to verify all configured LSP attribute lists. Use this task to display all LSP attribute lists to verify that the attributes lists that you configured are in operation.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng lsp attributes [*string*] [details]**
3. **show running-config | begin *text-string***
4. **exit**

### DETAILED STEPS

**Step 1**    **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

**Step 2**    **show mpls traffic-eng lsp attributes [*string*] [details]**

Use this command to verify that all configured LSP attribute lists are as expected. For example:

```
Router# show mpls traffic-eng lsp attributes
```

```

LIST 1
  affinity 1 mask 1
  bandwidth 1000
  priority 1 1
LIST 2
  bandwidth 5000
LIST hipriority
  priority 0 0
!
```

**Step 3**    **show running-config | begin *text-string***

Use this command to verify that all configured LSP attribute lists are as expected. Use the **begin** command modifier with the **mpls traffic-eng lsp *text-string*** to locate the LSP attributes information in the configuration file. For example:

```

Router# show running-config | begin mpls traffic-eng lsp

mpls traffic-eng lsp attributes 1
  affinity 1 mask 1
  bandwidth 1000
  priority 1 1
!
mpls traffic-eng lsp attributes 2
  bandwidth 5000
!
mpls traffic-eng lsp attributes hipriority
  priority 0 0
.
.
.
Router#
```

**Step 4**    **exit**

Use this command to exit to user EXEC mode. For example:

```

Router# exit
Router>
```

## Associating an LSP Attribute List with a Path Option for an MPLS TE Tunnel

Perform this task to associate an LSP attribute list with a path option for an MPLS TE tunnel. This task is required if you want to apply the LSP attribute list that you configured to path options for your MPLS TE tunnels.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

### Default Path Option Attributes for TE Tunnels Using LSP Attribute Lists

Values for path option attributes for a TE tunnel are determined in this manner:

- LSP attribute list values referenced by the path option take precedence over the values configured on the tunnel interface.

- If an attribute is not specified in the LSP attribute list, the device uses the attribute in the tunnel configuration. LSP attribute lists do not have defaults.
- If the attribute is not configured on the tunnel, then the device uses the tunnel default value, as follows:
 

```
{ affinity= affinity 0 mask 0,
  auto-bw= no auto-bw,
  bandwidth= bandwidth 0,
  lockdown= no lockdown,
  priority= priority 7 7,
  protection fast-reroute= no protection fast-reroute,
  record-route= no record-route
.
.
.
}
```

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mode mpls traffic-eng**
6. **tunnel mpls traffic-eng autoroute announce**
7. **tunnel mpls traffic-eng bandwidth** [**sub-pool** | **global**] *kbps*
8. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
9. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**] } [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
10. **end**

## DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>interface</b> <i>type number</i></p> <p><b>Example:</b><br/>Router(config)# interface tunnel 1</p>                                                                                | <p>Configures an interface type and enters interface configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface that you want to configure.</li> <li>The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 4 | <p><b>tunnel destination</b> {<i>hostname</i>   <i>ip-address</i>}</p> <p><b>Example:</b><br/>Router(config-if)# tunnel destination 10.10.10.12</p>                                     | <p>Specifies the destination of the tunnel for this path option.</p> <ul style="list-style-type: none"> <li>The <i>hostname</i> argument is the name of the host destination.</li> <li>The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 5 | <p><b>tunnel mode mpls traffic-eng</b></p> <p><b>Example:</b><br/>Router(config-if)# tunnel mode mpls traffic-eng</p>                                                                   | <p>Sets the encapsulation mode for the tunnel for MPLS TE.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | <p><b>tunnel mpls traffic-eng autoroute announce</b></p> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng autoroute announce</p>                                       | <p>Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 7 | <p><b>tunnel mpls traffic-eng bandwidth</b> [<i>sub-pool</i>   <i>global</i>] <i>bandwidth</i></p> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng bandwidth 1000</p> | <p>Configures the bandwidth required for an MPLS TE tunnel and assigns it either to the subpool or the global pool.</p> <ul style="list-style-type: none"> <li>The <b>sub-pool</b> keyword indicates a subpool tunnel.</li> <li>The <b>global</b> keyword indicates a global pool tunnel. Entering this keyword is not necessary, for all tunnels are in the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295.</li> </ul>                                                                                                                                                                                |
| Step 8 | <p><b>tunnel mpls traffic-eng priority</b> <i>setup-priority</i> [<i>hold-priority</i>]</p> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng priority 1 1</p>          | <p>Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted.</p> <ul style="list-style-type: none"> <li>The <i>setup-priority</i> argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted.<br/><br/>Valid values are from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.</li> <li>The <i>hold-priority</i> argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled.<br/><br/>Valid values are from 0 to 7, where a lower number indicates a higher priority.</li> </ul> |

| Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 9</b></p> <pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [sub-pool   global] kbps] [lockdown]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>path-option 1 dynamic attributes 1</p> | <p>Adds an LSP attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the path option.</li> <li>The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>The <b>name path-name</b> keyword argument combination identifies the name of the explicit path option.</li> <li>The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>The <b>attributes string</b> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| <p><b>Step 10</b></p> <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                                                                                                     | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



## Modifying a Path Option to Use a Different LSP Attribute List

Perform this task to modify the path option to use a different LSP attribute list.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options or change the set of attributes associated with a path option. You use the **tunnel mpls traffic-eng path-option** *number* **dynamic attributes** *string* command in interface configuration mode to modify the path option to use a different LSP attribute list. The **attributes** *string* keyword and argument names the new LSP attribute list for the path option specified.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [*sub-pool* | **global**] *kbits*] [**lockdown**]
6. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                              | Configures the interface type and enters interface configuration mode.<br><ul style="list-style-type: none"> <li>• The <i>type</i> argument is the type of interface that you want to configure.</li> <li>• The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li> </ul>  |
| Step 4 | <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12 | Specifies the destination of the tunnel for this path option.<br><ul style="list-style-type: none"> <li>• The <i>hostname</i> argument is the name of the host destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li> </ul> |

| Command or Action                                                                                                                                                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 5</b></p> <pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [sub-pool   global] kbps] [lockdown]</pre> <p><b>Example:</b></p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1</pre> | <p>Adds an LSP attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the path option.</li> <li>The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>The <b>name path-name</b> keyword argument combination identifies the name of the explicit path option.</li> <li>The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>The <b>attributes string</b> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| <p><b>Step 6</b></p> <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config-if)# end</pre>                                                                                                                                                                                                                                  | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Removing a Path Option for an LSP for an MPLS TE Tunnel

Perform this task to remove a path option for an LSP for an MPLS TE tunnel. Use this task to remove a path option for an LSP when your MPLS TE tunnel traffic requirements change.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **no tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbits*] [**lockdown**]
6. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                              | Configures the interface type and enters interface configuration mode.<br><ul style="list-style-type: none"><li>• The <i>type</i> argument is the type of interface that you want to configure.</li><li>• The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li></ul>  |
| Step 4 | <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12 | Specifies the destination of the tunnel for this path option.<br><ul style="list-style-type: none"><li>• The <i>hostname</i> argument is the name of the host destination.</li><li>• The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li></ul> |

| Command or Action                                                                                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 5</b></p> <pre>no tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [sub-pool   global] kbps] [lockdown]</pre> <p><b>Example:</b><br/>Router(config-if)# no tunnel mpls traffic-eng<br/>path-option 1 dynamic attributes 1</p> | <p>Removes an LSP attribute list that specifies LSP-related parameters for a path option for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the path option.</li> <li>• The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>• The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>• The <b>name path-name</b> keyword argument combination identifies the name of the explicit path option.</li> <li>• The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>• The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>• The <b>attributes string</b> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>• The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>• The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>• The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>• The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>• The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| <p><b>Step 6</b></p> <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                                                                                                            | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Verifying that LSP Is Signaled Using the Correct Attributes

Perform this task to verify that the LSP is signaled using the correct attributes.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels *tunnel-interface* [brief]**
3. **exit**

### DETAILED STEPS

---

**Step 1 enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

**Step 2 show mpls traffic-eng tunnels *tunnel-interface* [brief]**

Use this command to verify that the LSP is signaled using the correct attributes for the specified tunnel. For example:

```
Router# show mpls traffic-eng tunnels tunnel1

Name: Router-10-c_t1                               (Tunnel1) Destination: 10.10.10.12
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected

  path option 2, type explicit path2 (Basis for Setup, path weight 65834)

Config Parameters:
  Bandwidth: 1000      kbps (Global)  Priority: 1 1  Affinity: 0x0/0xFFFF
  Metric Type: IGP (global)
  AutoRoute: enabled   LockDown: disabled Loadshare: 1      bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 2 is active
  BandwidthOverride: enabled   LockDown: disabled Verbatim: disabled

Bandwidth Override:
  Signalling: 1        kbps (Global)
  Overriding: 1000     kbps (Global) configured on tunnel
```

The output shows that the following attributes are signaled for tunnel tunnel1: affinity 0 mask 0, auto-bw disabled, bandwidth 1000, lockdown disabled, and priority 1 1.

**Step 3 exit**

Use this command to return to user EXEC mode. For example:

```
Router# exit
Router>
```

---

## Configuring a Path Option for Bandwidth Override

This section contains the following tasks for configuring a path option for bandwidth override:

- [Configuring Fallback Bandwidth Path Options for TE Tunnels, page 26](#) (required)
- [Modifying the Bandwidth on a Path Option for Bandwidth Override, page 29](#) (optional)
- [Removing a Path Option for Bandwidth Override, page 31](#) (optional)
- [Verifying that LSP Is Signaled Using the Correct Bandwidth, page 33](#) (optional)



### Note

Once you configure bandwidth as a path-option parameter, you can no longer configure an LSP attribute list as a path-option parameter.

## Configuring Fallback Bandwidth Path Options for TE Tunnels

Perform this task to configure fallback bandwidth path options for a TE tunnel. Use this task to configure path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

Configuration of the Path Option for Bandwidth Override feature can reduce bandwidth constraints on path options temporarily and improve the chances that an LSP is set up for the TE tunnel. When a TE tunnel uses a path option with bandwidth override, the traffic engineering software attempts every 30 seconds to reoptimize the tunnel to use the preferred path option with the original configured bandwidth. The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the **mpls traffic-eng reoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path--name* | *path-number*} [**verbatim**] } [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**

## DETAILED STEPS

|        | Command or Action                                                                 | Purpose                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                         |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                                 |                                                                                                                                                                                                                                                        |
| Step 2 | <code>configure terminal</code>                                                   | Enters global configuration mode.                                                                                                                                                                                                                      |
|        | <b>Example:</b><br><code>Router# configure terminal</code>                        |                                                                                                                                                                                                                                                        |
| Step 3 | <code>interface type number</code>                                                | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                  |
|        | <b>Example:</b><br><code>Router(config)# interface tunnel 1</code>                | <ul style="list-style-type: none"><li>The <i>type</i> argument is the type of interface that you want to configure.</li><li>The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li></ul>           |
| Step 4 | <code>tunnel destination {hostname   ip-address}</code>                           | Specifies the destination of the tunnel for this path option.                                                                                                                                                                                          |
|        | <b>Example:</b><br><code>Router(config-if)# tunnel destination 10.10.10.12</code> | <ul style="list-style-type: none"><li>The <i>hostname</i> argument is the name of the host destination.</li><li>The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li></ul> |

| Command or Action                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 5</b></p> <pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [sub-pool   global] kbps] [lockdown]</pre> <p><b>Example:</b></p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic bandwidth 500</pre> | <p>Adds a path option for bandwidth override to specify a bandwidth fallback for a path option for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>• The <i>number</i> argument identifies the path option.</li> <li>• The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>• The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>• The <b>name</b> <i>path-name</i> keyword argument combination identifies the name of the explicit path option.</li> <li>• The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>• The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>• The <b>attributes</b> <i>string</i> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>• The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>• The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>• The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>• The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>• The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| <p><b>Step 6</b></p> <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config-if)# end</pre>                                                                                                                                                                                                                                   | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



## Modifying the Bandwidth on a Path Option for Bandwidth Override

Perform this task to modify the bandwidth on a path option for bandwidth override. You might need to further reduce or modify the bandwidth constraint for a path option to ensure that the headend of a tunnel establishes an LSP.

The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the **mpls traffic-eng reoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [*sub-pool* | **global**] *kbps*] [**lockdown**]
6. **end**
7. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                              | Configures the interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument is the type of interface that you want to configure.</li> <li>• The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li> </ul>  |
| Step 4 | <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12 | Specifies the destination of the tunnel for this path option. <ul style="list-style-type: none"> <li>• The <i>hostname</i> argument is the name of the host destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>tunnel mpls traffic-eng path-option</b> <i>number</i> {<b>dynamic</b>   <b>explicit</b> {<b>name</b> <i>path-name</i>   <i>path-number</i>} [<b>verbatim</b>] } [<b>attributes</b> <i>string</i>] [<b>bandwidth</b> [<b>sub-pool</b>   <b>global</b>] <i>kbps</i>] [<b>lockdown</b>]</p> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500</p> | <p>Adds a path option for bandwidth override to specify a bandwidth fallback for a path option for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the path option.</li> <li>The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>The <b>name</b> <i>path-name</i> keyword argument combination identifies the name of the explicit path option.</li> <li>The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>The <b>attributes</b> <i>string</i> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| Step 6 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                                                                                                                                                                                                      | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | <p><b>show mpls traffic-eng tunnels</b> <i>tunnel-interface</i> [<b>brief</b>]</p> <p><b>Example:</b><br/>Router# show mpls traffic-eng tunnels tunnel1</p>                                                                                                                                                                                                                                              | <p>(Optional) Displays information about tunnels.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls traffic-eng tunnels</b> command to verify which bandwidth path option is in use by the LSP.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Removing a Path Option for Bandwidth Override

Perform this task to remove the bandwidth on the path option for bandwidth override. The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. Use this task to remove the bandwidth override when it is not required.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **no tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**
7. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

### DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                              | Configures an interface type and enters interface configuration mode.<br><ul style="list-style-type: none"> <li>• The <i>type</i> argument is the type of interface that you want to configure.</li> <li>• The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.</li> </ul>   |
| Step 4 | <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12 | Specifies the destination of the tunnel for this path option.<br><ul style="list-style-type: none"> <li>• The <i>hostname</i> argument is the name of the host destination.</li> <li>• The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>no tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number} [verbatim]} [attributes string] [bandwidth [sub-pool   global] kbps] [lockdown]</pre> <p><b>Example:</b><br/>Router(config-if)# no tunnel mpls traffic-eng<br/>path-option 2 dynamic bandwidth 500</p> | <p>Removes a path option for bandwidth override that specifies a bandwidth fallback for a path option for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the path option.</li> <li>The <b>dynamic</b> keyword indicates that the path option is dynamically calculated (the router figures out the best path).</li> <li>The <b>explicit</b> keyword indicates that the path option is specified. You specify the IP addresses of the path.</li> <li>The <b>name path-name</b> keyword argument combination identifies the name of the explicit path option.</li> <li>The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>The <b>attributes string</b> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>The <b>bandwidth</b> keyword specifies LSP bandwidth.</li> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <b>global</b> keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the <b>sub-pool</b> keyword.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| Step 6 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                                                                                                             | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | <pre>show mpls traffic-eng tunnels tunnel-interface [brief]</pre> <p><b>Example:</b><br/>Router# show mpls traffic-eng tunnels tunnel1</p>                                                                                                                                                                   | <p>(Optional) Displays information about tunnels.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls traffic-eng tunnels</b> command to verify which bandwidth path option is in use by the LSP.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Verifying that LSP Is Signaled Using the Correct Bandwidth

Perform this task to verify that the LSP is signaled with the correct bandwidth.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels *tunnel-interface* [brief]**
3. **exit**

### DETAILED STEPS

#### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

#### Step 2 **show mpls traffic-eng tunnels *tunnel-interface* [brief]**

Use this command to verify that the LSP is signaled with the correct bandwidth and to verify that the bandwidth configured on the tunnel is overridden. For example:

```
Router# show mpls traffic-eng tunnels tunnel121

Name: Router-15-c_t21                               (Tunnel121) Destination: 10.10.10.12
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected

  path option 2, type explicit path2 (Basis for Setup, path weight 65834)
  path option 1, type explicit path1

Config Parameters:
  Bandwidth: 1000      kbps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
  Metric Type: IGP (global)
  AutoRoute: enabled LockDown: disabled Loadshare: 1 bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 2 is active
  BandwidthOverride: enabled LockDown: disabled Verbatim: disabled

Bandwidth Override:
  Signalling: 500 kbps (Global)
  Overriding: 1000      kbps (Global) configured on tunnel
```

If bandwidth override is actively being signaled, the **show mpls traffic-eng tunnel** command displays the bandwidth override information under the Active Path Option Parameters heading. The example shows that BandwidthOverride is enabled and that the tunnel is signaled using path-option 2. The bandwidth signaled is 500. This is the value configured on the path option 2 and it overrides the 1000 kbps bandwidth configured on the tunnel interface.

#### Step 3 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Troubleshooting Tips

If the tunnel state is down and you configured a path-option with bandwidth override enabled, the **show mpls traffic-eng tunnels** command indicates other reasons why a tunnel is not established. For example:

- The tunnel destination is not in the routing table.
- If the bandwidth override value is not zero, the bandwidth constraint may still be too large.
- Other attributes configured on the tunnel, such as affinity, might prevent the calculation of a path over the existing topology.
- TE might not be configured on all links necessary to reach tunnel destination.

# Configuration Examples for MPLS Traffic Engineering—LSP Attributes

This section contains the following configuration examples for the MPLS Traffic Engineering—LSP Attributes features:

- [Configuring LSP Attribute List: Examples, page 34](#)
- [Configuring a Path Option for Bandwidth Override: Examples, page 37](#)

## Configuring LSP Attribute List: Examples

This section contains the following examples for configuring LSP attribute lists:

- [Configuring an LSP Attribute List: Example, page 34](#)
- [Adding Attributes to an LSP Attribute List: Example, page 35](#)
- [Removing an Attribute from an LSP Attribute List: Example, page 35](#)
- [Modifying an Attribute in an LSP Attribute List: Example, page 35](#)
- [Deleting an LSP Attribute List: Example, page 35](#)
- [Associating an LSP Attribute List with a Path Option for a TE Tunnel: Example, page 36](#)
- [Modifying a Path Option to Use a Different LSP Attribute List: Example, page 36](#)
- [Removing a Path Option for Bandwidth Override: Example, page 39](#)

## Configuring an LSP Attribute List: Example

This example shows the configuration of the affinity, bandwidth, and priority LSP-related attributes in an LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
```

## Adding Attributes to an LSP Attribute List: Example

This example shows the addition of protection attributes to the LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# protection fast-reroute
Router(config-lsp-attr)# exit
```

## Removing an Attribute from an LSP Attribute List: Example

The following example shows removing the priority attribute from the LSP attribute list identified by the string simple:

```
Router(config)# mpls traffic-eng lsp attributes simple
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list

LIST simple
  priority 1 1
!
Router(config-lsp-attr)# no priority
Router(config-lsp-attr)# list

LIST simple
!
Router(config-lsp-attr)# exit
```

## Modifying an Attribute in an LSP Attribute List: Example

The following example shows modifying the bandwidth in an LSP attribute list identified by the numeral 5:

```
Router(config)# mpls traffic-eng lsp attributes 5
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list

LIST 5
  bandwidth 1000
  priority 1 1

Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# list

LIST 5
  bandwidth 500
  priority 1 1

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

## Deleting an LSP Attribute List: Example

The following example shows the deletion of an LSP attribute list identified by numeral 1:

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

```

Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
!
Router(config)# no mpls traffic-eng lsp attributes 1

```

## Associating an LSP Attribute List with a Path Option for a TE Tunnel: Example

The following example associates the LSP attribute list identified by the numeral 3 with path option 1:

```

Router(config)# mpls traffic-eng lsp attributes 3
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 2 2
Router(config-lsp-attr)# protection fast-reroute
Router(config-lsp-attr)# exit
!
!
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered Ethernet4/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 3

```

In this configuration, the LSP will have the following attributes:

```

{bandwidth = 1000
 priority = 2 2
 affinity 1
 reroute enabled.
}

```

The LSP attribute list referenced by the path option will take precedence over the values configured on the tunnel interface.

## Modifying a Path Option to Use a Different LSP Attribute List: Example

The following example modifies path option 1 to use an LSP attribute list identified by the numeral 1:

```

Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit

Router(config)# mpls traffic-eng lsp attributes 2
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit

Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered Ethernet4/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1

```

In this configuration, the LSP will have the following attributes:

```

{affinity = 7 7

```



```
bandwidth = 500
priority = 1 1
}
```

## Removing a Path Option for an LSP for an MPLS TE Tunnel: Example

The following example shows the removal of path option 1 for an LSP for a TE tunnel:

```
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered Ethernet4/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
Router(config-if)# tunnel mpls traffic-eng path-option 2 explicit path2 attributes 2
!
!
Router(config-if)# no tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
```

## Configuring a Path Option for Bandwidth Override: Examples

This section contains the following examples for configuring a path option for bandwidth override:

- [Path Option for Bandwidth Override and LSP Attribute List Configuration Command Examples, page 37](#)
- [Configuring Fallback Bandwidth Path Options for TE Tunnels: Example, page 38](#)
- [Modifying the Bandwidth on a Path Option for Bandwidth Override: Example, page 38](#)
- [Removing a Path Option for Bandwidth Override: Example, page 39](#)

## Path Option for Bandwidth Override and LSP Attribute List Configuration Command Examples

The following are examples of the Cisco IOS command-line interface (CLI) to use when you configure a path option to override the bandwidth:

```
Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 ?

attributes Specify an LSP attribute list
bandwidth  override the bandwidth configured on the tunnel
lockdown    not a candidate for reoptimization
<cr>

Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth ?

<0-4294967295>  bandwidth requirement in kbps
sub-pool        tunnel uses sub-pool bandwidth

Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth 500
?
lockdown    not a candidate for reoptimization
<cr>
```



### Note

Once you configure bandwidth as a path-option parameter, you can no longer configure an LSP attribute list as a path-option parameter.

## Configuring Fallback Bandwidth Path Options for TE Tunnels: Example

The following example shows multiple path options configured with the **tunnel mpls traffic-eng path-option** command:

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
end
```

The device selects a path option for an LSP in order of preference, as follows:

- The device attempts to signal an LSP using path options starting with path-option 1.  
The device attempts to signal an LSP with the 1000 kbps bandwidth configured on the tunnel interface because path-option 1 has no bandwidth configured.
- If 1000 kbps bandwidth is not available over the network, the device attempts to establish an LSP using path-option 2.  
Path-option 2 has a bandwidth of 500 kbps configured. This reduces the bandwidth constraint from the original 1000 kbps configured on the tunnel interface.
- If 500 kbps is not available, the device attempts to establish an LSP using path-option 3.  
Path-option 3 is configured as dynamic and has bandwidth 0. The device establishes the LSP if an IP path exists to the destination and all other tunnel constraints are met.

## Modifying the Bandwidth on a Path Option for Bandwidth Override: Example

The following example shows modifying the bandwidth on a path option for bandwidth override. Path-option 3 is changed to an explicit path with a bandwidth of 100 kbps. Path-option 4 is configured with bandwidth 0.

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
!
!
Router(config)# tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
Router(config)# tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
```

## Removing a Path Option for Bandwidth Override: Example

The following example shows removing a path option for bandwidth override:

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
 tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
!
Router(config)# no tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—LSP Attributes feature.

## Related Documents

| Related Topic                                                             | Document Title                                                                              |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| MPLS TE automatic bandwidth adjustment for TE tunnels configuration tasks | <a href="#">MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels</a> |
| MPLS TE command descriptions                                              | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                   |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **affinity (LSP Attributes)**
- **auto-bw (LSP Attributes)**
- **bandwidth (LSP Attributes)**
- **exit (LSP Attributes)**
- **list (LSP Attributes)**
- **lockdown (LSP Attributes)**
- **mpls traffic-eng lsp attributes**
- **priority (LSP Attributes)**
- **protection (LSP Attributes)**
- **record-route (LSP Attributes)**
- **show mpls traffic-eng lsp attributes**
- **show mpls traffic-eng tunnels**

# Feature Information for MPLS Traffic Engineering—LSP Attributes

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering—LSP Attributes

| Feature Name                            | Releases                                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------|------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—LSP Attributes | 12.0(26)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T | <p>This document describes how to configure label switched path (LSP) attributes for path options associated with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.</p> <p>The MPLS Traffic Engineering—LSP Attributes feature is an extension to MPLS TE that provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features provide flexibility in the configuration of LSP attributes for MPLS TE tunnel path options. Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a path option for bandwidth override.</p> <p>In 12.0(26)S, this feature was introduced.</p> <p>In 12.2(33)SRA, this feature was integrated into a Cisco IOS 12.2SRA release.</p> <p>In 12.2(33)SXH, this feature was integrated into a Cisco IOS 12.2SXH release.</p> <p>In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS Traffic Engineering—LSP Attributes Benefits, page 2</a></li> <li>• <a href="#">Traffic Engineering Bandwidth and Bandwidth Pools, page 3</a></li> </ul> |

**Table 1**      *Feature Information for MPLS Traffic Engineering—LSP Attributes (continued)*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <ul style="list-style-type: none"> <li>• <a href="#">LSP Attribute Lists Usage and Management</a>, page 3</li> <li>• <a href="#">Autobandwidth and Path Option for Bandwidth Override</a>, page 4</li> <li>• <a href="#">Path Option Selection for MPLS TE Tunnel LSPs</a>, page 5</li> <li>• <a href="#">Configuring MPLS Traffic Engineering LSP Attribute Lists</a>, page 6</li> <li>• <a href="#">Configuring a Path Option for Bandwidth Override</a>, page 26</li> </ul> <p>The following commands were introduced or modified: <b>affinity</b> (LSP Attributes), <b>auto-bw</b> (LSP Attributes), <b>bandwidth</b> (LSP Attributes), <b>exit</b> (LSP Attributes), <b>list</b> (LSP Attributes), <b>lockdown</b> (LSP Attributes), <b>mpls traffic-eng lsp attributes</b>, <b>priority</b> (LSP Attributes), <b>protection</b> (LSP Attributes), <b>record-route</b> (LSP Attributes), <b>show mpls traffic-eng lsp attributes</b>, and <b>show mpls traffic-eng tunnels</b>.</p> |

# Glossary

**bandwidth**—The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.

**bandwidth reservation**—The process of assigning bandwidth to users and applications served by a network. This process involves assigning priority to different flows of traffic based on how critical and delay-sensitive they are. This makes the best use of available bandwidth, and if the network becomes congested, lower-priority traffic can be dropped. Sometimes called bandwidth allocation

**global pool**—The total bandwidth allocated to an MPLS traffic engineering link.

**label switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**LSR**—label switch router. A Multiprotocol Label Switching (MPLS) node that can forward native Layer 3 packets. The LSR forwards a packet based on the value of a label attached to the packet.

**MPLS TE**—MPLS traffic engineering (formerly known as “RRR” or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

**subpool**—The more restrictive bandwidth in an MPLS traffic engineering link. The subpool is a portion of the link's overall global pool bandwidth.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used. The application of scientific principles and technology to measure, model, and control internet traffic in order to simultaneously optimize traffic performance and network resource utilization.

**traffic engineering tunnel**—A label-switched tunnel used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

**tunnel**—A secure communication path between two peers, such as two routers.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2003—2009 Cisco Systems, Inc. All rights reserved.







# MPLS Traffic Engineering—Autotunnel Primary and Backup

---

**First Published:** January 26, 2004  
**Last Updated:** October 21, 2009

The MPLS Traffic Engineering—Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

A router with primary one-hop autotunnels and backup autotunnels can be configured with stateful switchover (SSO) redundancy.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering—Autotunnel Primary and Backup” section on page 17](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—Autotunnel Primary and Backup, page 2](#)
- [Restrictions for MPLS Traffic Engineering—Autotunnel Primary and Backup, page 2](#)
- [Information About MPLS Traffic Engineering—Autotunnel Primary and Backup, page 2](#)
- [How to Configure MPLS Traffic Engineering—Autotunnel Primary and Backup, page 8](#)
- [Configuration Examples for MPLS Traffic Engineering—Autotunnel Primary and Backup, page 11](#)



---

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

- [Additional References, page 15](#)
- [Feature Information for MPLS Traffic Engineering—Autotunnel Primary and Backup, page 17](#)
- [Glossary, page 18](#)

## Prerequisites for MPLS Traffic Engineering—Autotunnel Primary and Backup

- Configure TE on the routers.

## Restrictions for MPLS Traffic Engineering—Autotunnel Primary and Backup

- You cannot configure a static route to route traffic over TE autotunnels. For autotunnels, you should use only the autoroute for tunnel selection.

## Information About MPLS Traffic Engineering—Autotunnel Primary and Backup

To configure autotunnels, you need to understand the following concepts:

- [Overview of MPLS Traffic Engineering—Autotunnel Primary and Backup, page 2](#)
- [Benefits of MPLS Traffic Engineering—Autotunnel Primary and Backup Feature, page 3](#)
- [MPLS Traffic Engineering, page 3](#)
- [MPLS Traffic Engineering Backup Autotunnels, page 3](#)
- [MPLS Traffic Engineering Primary Autotunnels, page 5](#)
- [MPLS Traffic Engineering Label-Based Forwarding, page 6](#)
- [Benefits of MPLS Traffic Engineering Protection, page 6](#)
- [SSO Redundancy Overview, page 7](#)

## Overview of MPLS Traffic Engineering—Autotunnel Primary and Backup

The MPLS Traffic Engineering—Autotunnel Primary and Backup feature has the following features:

- Backup autotunnel—Enables a router to dynamically build backup tunnels.
- Primary one-hop autotunnel—Enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

If no backup tunnels exist, the following types of backup tunnels are created:

- Next hop (NHOP)
- Next-next hop (NNHOP)

## Benefits of MPLS Traffic Engineering—Autotunnel Primary and Backup Feature

- Backup tunnels are built automatically, eliminating the need for users to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface.
- The dynamic creation of one-hop primary tunnels eliminates the need to configure an MPLS TE tunnel with the Fast Reroute (FRR) option for the tunnel to be protected.
- Protection is expanded; FRR does not protect IP traffic that is not using the TE tunnel or Label Distribution Protocol (LDP) labels that are not using the TE tunnel.

## MPLS Traffic Engineering

MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

TE is the process of adjusting bandwidth allocations to ensure that enough bandwidth is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then sets the bandwidth available for that tunnel.

## MPLS Traffic Engineering Backup Autotunnels

MPLS backup autotunnels protect fast reroutable TE label switched paths (LSPs). Without MPLS backup autotunnels to protect a LSP you had to do the following:

- Preconfigure each backup tunnel.
- Assign the backup tunnels to the protected interfaces.

An LSP requests backup protection from Resource Reservation Protocol (RSVP) FRR in the following situations:

- Receipt of the first RSVP Resv message
- Receipt of an RSVP path message with the protection attribute after the LSP has been established without the protection attribute
- Detection that a Record Route Object (RRO) changed

If there was no backup tunnel protecting the interface used by the LSP, the LSP remained unprotected.

Backup autotunnels enable a router to dynamically build backup tunnels when they are needed. This prevents you from having to build MPLS TE tunnels statically.

Backup tunnels may not be available for the following reasons:

- Static backup tunnels are not configured.
- Static backup tunnels are configured, but cannot protect the LSP. The backup tunnel may not have enough available bandwidth, the tunnel may protect a different pool, or the tunnel may be down.

If a backup tunnel is not available, the following two backup tunnels are created dynamically:

- NHOP—Protects against link failure
- NNHOP—Protects against node failure

**Note**

At the penultimate hop, only an NHOP backup tunnel is created.

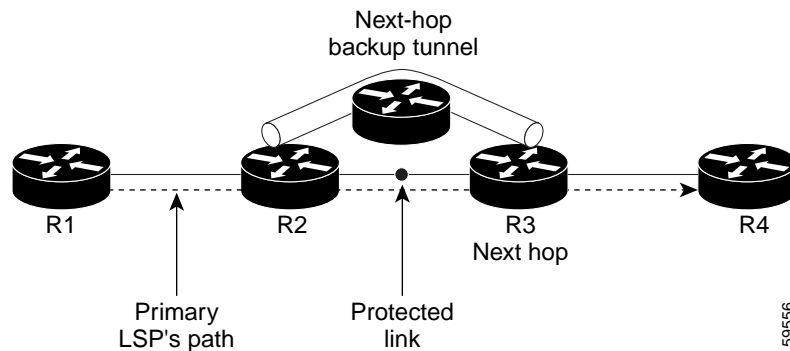
**Note**

If two LSPs share the same output interface and NHOP, three (not four) backup tunnels are created. They share an NHOP backup tunnel.

## Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as NHOP backup tunnels because they terminate at the LSP's next hop beyond the point of failure. [Figure 1](#) illustrates an NHOP backup tunnel.

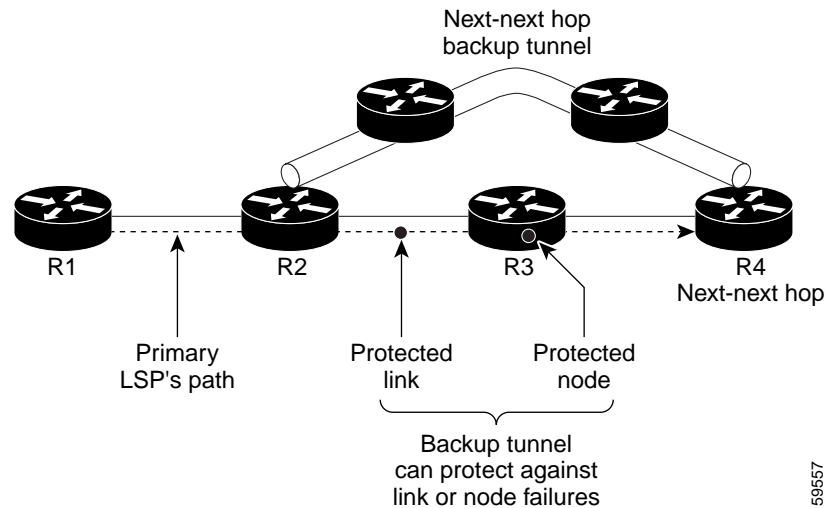
**Figure 1**      *Next-Hop Backup Tunnel*



## Node Protection

Backup tunnels that bypass next-hop nodes along LSP paths are called NNHOP backup tunnels because they terminate at the node following the next-hop node of the LSPs, thereby bypassing the next-hop node. They protect LSPs by enabling the node upstream of a link or node failure to reroute the LSPs and their traffic around the failure to the next-hop node. NNHOP backup tunnels also provide protection from link failures because they bypass the failed link and the node.

[Figure 2](#) illustrates an NNHOP backup tunnel.

**Figure 2**      **Next-Next Hop Backup Tunnel**

59557

## Explicit Paths

Explicit paths are used to create backup autotunnels as follows:

- NHOP excludes the protected link's IP address.
- NNHOP excludes the NHOP router ID.
- The explicit-path name is `_auto-tunnel_tunnelxxx`, where `xxx` matches the dynamically created backup tunnel ID.
- The interface used for the `ip unnumbered` command defaults to Loopback0. You can configure this to use a different interface.

## Range for Backup Autotunnels

The tunnel range for backup autotunnels is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 1000 to 1100 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the MPLS TE dynamic tunnel software can use those IDs.

## MPLS Traffic Engineering Primary Autotunnels

The MPLS Traffic Engineering—Autotunnel Primary and Backup feature enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS traffic. The tunnels are created with zero bandwidth. The constraint-based shortest path first (CSPF) is the same as the shortest path first (SPF) when there is zero bandwidth, so the router's choice of the autorouted one-hop primary tunnel is the same as if there were no tunnel. Because it is a one-hop tunnel, the encapsulation is tag-implicit (that is, there is no tag header).

## Explicit Paths

Explicit paths are used to create autotunnels as follows:

- The explicit path is dynamically created.
- The explicit path includes the IP address for the interface connected to the next hop.
- The explicit-path name is `_auto-tunnel_tunnelxxx`, where `xxx` matches the dynamically created one-hop tunnel ID.
- Interfaces used for the **ip unnumbered** command default to Loopback0. You can configure this to use a different interface.

## Range for Autotunnels

The tunnel range is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 100 to 200 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the IDs become available for use by the MPLS TE dynamic tunnel software.

## MPLS Traffic Engineering Label-Based Forwarding

Routers receive a packet, determine where it needs to go by examining some fields in the packet, and send it to the appropriate output device. A label is a short, fixed-length identifier that is used to forward packets. A label switching device normally replaces the label in a packet with a new value before forwarding the packet to the next hop. For this reason, the forwarding algorithm is called label swapping. A label switching device, referred to as an LSR, runs standard IP control protocols (that is, routing protocols, RSVP, and so forth) to determine where to forward packets.

## Benefits of MPLS Traffic Engineering Protection

The following sections describe the benefits of MPLS traffic engineering protection:

- [Delivery of Packets During a Failure, page 6](#)
- [Multiple Backup Tunnels Protecting the Same Interface, page 6](#)
- [Scalability, page 7](#)
- [RSVP Hello, page 7](#)

### Delivery of Packets During a Failure

Backup tunnels that terminate at the NNHOP protect both the downstream link and node. This provides protection for link and node failures.

### Multiple Backup Tunnels Protecting the Same Interface

In addition to being required for node protection, the autotunnel primary and backup feature provides the following benefits:

- Redundancy—If one backup tunnel is down, other backup tunnels protect LSPs.
- Increased backup capacity—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels).

## Scalability

A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

An example of N:1 protection is that when one backup tunnel protects 5000 LSPs, each router along the backup path maintains one additional tunnel.

An example of 1:1 protection is that when 5000 backup tunnels protect 5000 LSPs, each router along the backup path must maintain state for an additional 5000 tunnels.

## RSVP Hello

RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, Hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

## SSO Redundancy Overview

The SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

SSO is particularly useful at the network edge. It provides protection for network edge devices with dual route processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizes critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

# How to Configure MPLS Traffic Engineering—Autotunnel Primary and Backup

This sections contains the following procedures:

- [Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs, page 8](#) (required)
- [Establishing MPLS One-Hop Tunnels to All Neighbors, page 9](#) (required)

## Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs

To establish an MPLS backup autotunnel to protect fast reroutable TE LSPs, perform the following task.

  
**Note**

Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls traffic-eng auto-tunnel backup`
4. `mpls traffic-eng auto-tunnel backup nhop-only`
5. `mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]`
6. `mpls traffic-eng auto-tunnel backup timers removal unused sec`
7. `mpls traffic-eng auto-tunnel backup config unnumbered-interface interface`

### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                                   |                                                                                                                  |
| Step 2 | <code>configure terminal</code>                                                     | Enters global configuration mode.                                                                                |
|        | <b>Example:</b><br><code>Router# configure terminal</code>                          |                                                                                                                  |
| Step 3 | <code>mpls traffic-eng auto-tunnel backup</code>                                    | Automatically builds NHOP and NNHOP backup tunnels.                                                              |
|        | <b>Example:</b><br><code>Router(config)# mpls traffic-eng auto-tunnel backup</code> |                                                                                                                  |



|        | Command or Action                                                                                                                                                                                      | Purpose                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>mpls traffic-eng auto-tunnel backup nhop-only</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel backup nhop-only                                                           | Enables the creation of dynamic NHOP backup tunnels.                                                       |
| Step 5 | <b>mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100                   | Configures the range of tunnel interface numbers for backup autotunnels.                                   |
| Step 6 | <b>mpls traffic-eng auto-tunnel backup timers removal unused sec</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50                            | Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used. |
| Step 7 | <b>mpls traffic-eng auto-tunnel backup config unnumbered-interface interface</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0 | Enables IP processing on the specified interface without an explicit address.                              |

## Establishing MPLS One-Hop Tunnels to All Neighbors

To establish MPLS one-hop tunnels to all neighbors, perform the following task.



### Note

Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel primary onehop**
4. **mpls traffic-eng auto-tunnel primary tunnel-num [min num] [max num]**
5. **mpls traffic-eng auto-tunnel primary timers removal rerouted sec**
6. **mpls traffic-eng auto-tunnel primary config unnumbered interface**
7. **mpls traffic-eng auto-tunnel primary config mpls ip**
8. **clear mpls traffic-eng auto-tunnel primary**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                      | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                         | Enters global configuration mode.                                                                                |
| Step 3 | <b>mpls traffic-eng auto-tunnel primary onehop</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel primary onehop                                               | Automatically creates primary tunnels to all next hops.                                                          |
| Step 4 | <b>mpls traffic-eng auto-tunnel primary tunnel-num [min num] [max num]</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100 | Configures the range of tunnel interface numbers for primary autotunnels.                                        |
| Step 5 | <b>mpls traffic-eng auto-tunnel primary timers removal rerouted sec</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 400     | Configures how many seconds after a failure primary autotunnels will be removed.                                 |
| Step 6 | <b>mpls traffic-eng auto-tunnel primary config unnumbered interface</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered ethernet1/0   | Enables IP processing on the specified interface without an explicit address.                                    |
| Step 7 | <b>mpls traffic-eng auto-tunnel primary config mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel primary config mpls ip                               | Enables LDP on primary autotunnels.                                                                              |
| Step 8 | <b>clear mpls traffic-eng auto-tunnel primary</b><br><br><b>Example:</b><br>Router(config)# clear mpls traffic-eng auto-tunnel primary                                                 | Removes all primary autotunnels and re-creates them.                                                             |

# Configuration Examples for MPLS Traffic Engineering—Autotunnel Primary and Backup

This section contains the following configuration examples:

- [Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs: Example, page 11](#)
- [Establishing MPLS One-Hop Tunnels to Neighbors: Example, page 13](#)

## Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs: Example



### Note

This example does not include the **mpls traffic-eng auto-tunnel backup nhop-only** command because autotunneling would not be able to create any backup tunnels.

To determine if there are any backup tunnels, enter the **show ip rsvp fast-reroute** command. This example shows that there is a static configured primary tunnel and no backup tunnels.

```
Router(config)# show ip rsvp fast-reroute
```

| Primary Tunnel | Protect I/F | BW BPS>Type | Backup Tunnel:Label | State | Level | Type  |
|----------------|-------------|-------------|---------------------|-------|-------|-------|
| -----          | -----       | -----       | -----               | ----- | ----- | ----- |
| R3-PRP_t0      | PO3/1       | 0:G         | None                | None  | None  |       |

The following command causes autotunnels to automatically configure NHOP and NNHOP backup tunnels:

```
Router(config)# mpls traffic-eng auto-tunnel backup
```

As illustrated in the **show ip interface brief** command output, autotunneling created two backup tunnels that have tunnel IDs 65436 and 65437:

```
Router# show ip interface brief
```

| Interface          | IP-Address | OK? | Method | Status                | Protocol |
|--------------------|------------|-----|--------|-----------------------|----------|
| POS2/0             | 10.0.0.14  | YES | NVRAM  | down                  | down     |
| POS2/1             | 10.0.0.49  | YES | NVRAM  | up                    | up       |
| POS2/2             | 10.0.0.45  | YES | NVRAM  | up                    | up       |
| POS2/3             | 10.0.0.57  | YES | NVRAM  | administratively down | down     |
| POS3/0             | 10.0.0.18  | YES | NVRAM  | down                  | down     |
| POS3/1             | 10.0.0.33  | YES | NVRAM  | up                    | up       |
| POS3/2             | unassigned | YES | NVRAM  | administratively down | down     |
| POS3/3             | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/0 | 10.0.0.37  | YES | NVRAM  | up                    | up       |
| GigabitEthernet4/1 | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/2 | unassigned | YES | NVRAM  | administratively down | down     |
| Loopback0          | 10.0.3.1   | YES | NVRAM  | up                    | up       |
| Tunnel0            | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65436        | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65437        | 10.0.3.1   | YES | unset  | up                    | up       |
| Ethernet0          | 10.3.38.3  | YES | NVRAM  | up                    | up       |
| Ethernet1          | unassigned | YES | NVRAM  | administratively down | down     |

The following command prevents autotunneling from creating NNHOP backup tunnels:

```
Router# mpls traffic-eng auto-tunnel backup nhop-only
```

The “Type” field in the following **show ip rsvp fast-reroute** command shows that there is only an NHOP tunnel:

```
Router# show ip rsvp fast-reroute
```

| Primary Tunnel | Protect I/F | BW BPS:Type | Backup Tunnel:Label | State | Level   | Type |
|----------------|-------------|-------------|---------------------|-------|---------|------|
| R3-PRP_t0      | PO3/1       | 0:G         | Tu65436:24          | Ready | any-unl | Nhop |

The following command changes the minimum and maximum tunnel interface numbers to 1000 and 1100, respectively:

```
Router# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100
```

You can verify the ID numbers and autotunnel backup range ID by entering the **show ip rsvp fast-reroute** and **show ip interface brief** commands. In this example, only one backup tunnel is protecting the primary tunnel:

```
Router# show ip rsvp fast-reroute
```

| Primary Tunnel | Protect I/F | BW BPS:Type | Backup Tunnel:Label | State | Level   | Type |
|----------------|-------------|-------------|---------------------|-------|---------|------|
| R3-PRP_t0      | PO3/1       | 0:G         | Tu1000:24           | Ready | any-unl | Nhop |

```
Router# show ip interface brief
```

| Interface          | IP-Address | OK? | Method | Status                | Protocol |
|--------------------|------------|-----|--------|-----------------------|----------|
| POS2/0             | 10.0.0.14  | YES | NVRAM  | down                  | down     |
| POS2/1             | 10.0.0.49  | YES | NVRAM  | up                    | up       |
| POS2/2             | 10.0.0.45  | YES | NVRAM  | up                    | up       |
| POS2/3             | 10.0.0.57  | YES | NVRAM  | administratively down | down     |
| POS3/0             | 10.0.0.18  | YES | NVRAM  | down                  | down     |
| POS3/1             | 10.0.0.33  | YES | NVRAM  | up                    | up       |
| POS3/2             | unassigned | YES | NVRAM  | administratively down | down     |
| POS3/3             | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/0 | 10.0.0.37  | YES | NVRAM  | up                    | up       |
| GigabitEthernet4/1 | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/2 | unassigned | YES | NVRAM  | administratively down | down     |
| Loopback0          | 10.0.3.1   | YES | NVRAM  | up                    | up       |
| Tunnel0            | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65436        | 10.0.3.1   | YES | unset  | up                    | up       |
| Ethernet0          | 10.3.38.3  | YES | NVRAM  | up                    | up       |
| Ethernet1          | unassigned | YES | NVRAM  | administratively down | down     |

The default tunnel range for autotunnel backup tunnels is 65,436 through 65,535. The following **show ip rsvp fast-reroute** command changes the tunnel range IDs:

```
Router# show ip rsvp fast-reroute
```

| Primary Tunnel | Protect I/F | BW BPS:Type | Backup Tunnel:Label | State | Level   | Type   |
|----------------|-------------|-------------|---------------------|-------|---------|--------|
| R3-PRP_t0      | PO3/1       | 0:G         | Tu1001:0            | Ready | any-unl | N-Nhop |

The results are shown in the **show ip interface brief** command:

```
Router# show ip interface
```

```
Router# show ip interface brief
```

| Interface | UP-Address | OK? | Method | Status | Protocol |
|-----------|------------|-----|--------|--------|----------|
|-----------|------------|-----|--------|--------|----------|

|            |            |     |       |                       |      |
|------------|------------|-----|-------|-----------------------|------|
| POS2/0     | 10.0.0.14  | YES | NVRAM | down                  | down |
| POS2/1     | 10.0.0.49  | YES | NVRAM | up                    | up   |
| POS2/2     | 10.0.0.45  | YES | NVRAM | up                    | up   |
| POS2/3     | 10.0.0.57  | YES | NVRAM | up                    | up   |
| POS3/0     | 10.0.0.18  | YES | NVRAM | up                    | up   |
| POS3/1     | 10.0.0.33  | YES | NVRAM | up                    | up   |
| POS3/2     | unassigned | YES | NVRAM | administratively down | down |
| POS3/3     | unassigned | YES | NVRAM | administratively down | down |
| Loopback0  | 10.0.3.1   | YES | NVRAM | up                    | up   |
| Tunnel0    | 10.0.3.1   | YES | unset | up                    | up   |
| Tunnel1000 | 10.0.3.1   | YES | unset | up                    | up   |
| Tunnel1001 | 10.0.3.1   | YES | unset | up                    | up   |
| Ethernet0  | 10.3.38.3  | YES | NVRAM | up                    | up   |
| Ethernet1  | unassigned | YES | NVRAM | administratively down | down |

The following **mpls traffic-eng auto-tunnel backup timers removal unused** command specifies that a timer will scan backup autotunnels every 50 seconds and the timer will remove tunnels that are not being used:

```
Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50
```

The following **mpls traffic-eng auto-tunnel backup config unnumbered-interface** command enables IP processing on POS interface 3/1:

```
Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface POS3/1
```

To verify that IP processing is enabled on POS3/1, enter the **show interfaces tunnel** command:

```
Router# show interfaces tunnel 1001
```

```
Tunnel1001 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered. Using address of POS3/1 (10.0.0.33)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.0, destination 10.0.5.1
  Tunnel protocol/transport Label Switching, sequencing disabled
  Key disabled
  Checksumming of packets disabled
  Last input never, 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
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

## Establishing MPLS One-Hop Tunnels to Neighbors: Example

For autotunneling to automatically create primary tunnels to all next hops, you must enter the following command:

```
Router(config)# mpls traffic-eng auto-tunnel primary onehop
```

In this example there are four primary tunnels and no backup tunnels. To verify that configuration, enter the **show ip rsvp fast-reroute** command and the **show ip interface brief** command:

```
Router# show ip rsvp fast-reroute
```

| Primary<br>Tunnel | Protect<br>I/F | BW<br>BPS:Type | Backup<br>Tunnel:Label | State | Level | Type |
|-------------------|----------------|----------------|------------------------|-------|-------|------|
| R3-PRP_t65337     | PO2/2          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t65338     | PO3/1          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t65339     | Gi4/0          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t65336     | PO2/1          | 0:G            | None                   | None  | None  |      |

```
Router# show ip interface brief
```

| Interface          | IP-Address | OK? | Method | Status                | Protocol |
|--------------------|------------|-----|--------|-----------------------|----------|
| POS2/0             | 10.0.0.14  | YES | NVRAM  | down                  | down     |
| POS2/1             | 10.0.0.49  | YES | NVRAM  | up                    | up       |
| POS2/2             | 10.0.0.45  | YES | NVRAM  | up                    | up       |
| POS2/3             | 10.0.0.57  | YES | NVRAM  | administratively down | down     |
| POS3/0             | 10.0.0.18  | YES | NVRAM  | down                  | down     |
| POS3/1             | 10.0.0.33  | YES | NVRAM  | up                    | up       |
| POS3/2             | unassigned | YES | NVRAM  | administratively down | down     |
| POS3/3             | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/0 | 10.0.0.37  | YES | NVRAM  | up                    | up       |
| GigabitEthernet4/1 | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/2 | unassigned | YES | NVRAM  | administratively down | down     |
| Loopback0          | 10.0.3.1   | YES | NVRAM  | up                    | up       |
| Tunnel0            | 10.0.3.1   | YES | unset  | administratively down | down     |
| Tunnel65336        | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65337        | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65338        | 10.0.3.1   | YES | unset  | up                    | up       |
| Tunnel65339        | 10.0.3.1   | YES | unset  | up                    | up       |
| Ethernet0          | 10.3.38.3  | YES | NVRAM  | up                    | up       |
| Ethernet1          | unassigned | YES | NVRAM  | administratively down | down     |

The default tunnel range for primary autotunnels is 65,336 through 65,435. The following **mpls traffic-eng auto-tunnel primary tunnel-num** command changes the range to 2000 through 2100:

```
Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

The following sample output from the **show ip rsvp fast-reroute** command and the **show ip interface brief** command shows that the tunnel IDs are 2000, 2001, 2002, and 2003:

```
Router# show ip rsvp fast-reroute
```

| Primary<br>Tunnel | Protect<br>I/F | BW<br>BPS:Type | Backup<br>Tunnel:Label | State | Level | Type |
|-------------------|----------------|----------------|------------------------|-------|-------|------|
| R3-PRP_t2001      | PO2/2          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t2002      | PO3/1          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t2003      | Gi4/0          | 0:G            | None                   | None  | None  |      |
| R3-PRP_t2000      | PO2/1          | 0:G            | None                   | None  | None  |      |

```
Router# show ip interface brief
```

| Interface          | IP-Address | OK? | Method | Status                | Protocol |
|--------------------|------------|-----|--------|-----------------------|----------|
| POS2/0             | 10.0.0.14  | YES | NVRAM  | down                  | down     |
| POS2/1             | 10.0.0.49  | YES | NVRAM  | up                    | up       |
| POS2/2             | 10.0.0.45  | YES | NVRAM  | up                    | up       |
| POS2/3             | 10.0.0.57  | YES | NVRAM  | administratively down | down     |
| POS3/0             | 10.0.0.18  | YES | NVRAM  | down                  | down     |
| POS3/1             | 10.0.0.33  | YES | NVRAM  | up                    | up       |
| POS3/2             | unassigned | YES | NVRAM  | administratively down | down     |
| POS3/3             | unassigned | YES | NVRAM  | administratively down | down     |
| GigabitEthernet4/0 | 10.0.0.37  | YES | NVRAM  | up                    | up       |

|                    |            |     |       |                       |      |
|--------------------|------------|-----|-------|-----------------------|------|
| GigabitEthernet4/1 | unassigned | YES | NVRAM | administratively down | down |
| GigabitEthernet4/2 | unassigned | YES | NVRAM | administratively down | down |
| Loopback0          | 10.0.3.1   | YES | NVRAM | up                    | up   |
| Tunnel0            | 10.0.3.1   | YES | unset | administratively down | down |
| Tunnel2000         | 10.0.3.1   | YES | unset | up                    | up   |
| Tunnel2001         | 10.0.3.1   | YES | unset | up                    | up   |
| Tunnel2002         | 10.0.3.1   | YES | unset | up                    | up   |
| Tunnel2003         | 10.0.3.1   | YES | unset | up                    | up   |
| Ethernet0          | 10.3.38.3  | YES | NVRAM | up                    | up   |
| Ethernet1          | unassigned | YES | NVRAM | administratively down | down |

The following **mpls traffic-eng auto-tunnel primary timers** command specifies that a timer will scan backup autotunnels every 50 seconds and remove tunnels that are not being used:

```
Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 50
```

The following **mpls traffic-eng auto-tunnel primary config unnumbered** command enables IP processing on POS interface 3/1:

```
Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered POS3/1
```

To specify that autotunneling remove all primary autotunnels and re-create them, enter the following command:

```
Router(config)# clear mpls traffic-eng auto-tunnel primary
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—Autotunnel Primary and Backup feature.

## Additional References

| Related Topic                     | Document Title                                                                                                          |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Backup tunnels                    | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a> |
| Link protection                   | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a> |
| MPLS traffic engineering commands | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                               |
| SSO                               | <a href="#">Cisco IOS High Availability Configuration Guide</a>                                                         |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |



# Feature Information for MPLS Traffic Engineering—Autotunnel Primary and Backup

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering—Autotunnel Primary and Backup

| Feature Name                                           | Releases                                                            | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—Autotunnel Primary and Backup | 12.0(27)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T<br>12.2(33)SRE | <p>The MPLS Traffic Engineering—Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.</p> <p>In Cisco IOS Release 12.0(27)S, this feature was introduced.</p> <p>In Cisco IOS Release 12.2(33)SRA, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SXH, support was added.</p> <p>In Cisco IOS Release 12.4(20)T, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was integrated. A router with primary one-hop autotunnels and backup autotunnels can be configured with SSO redundancy.</p> |

# Glossary

**backup tunnel**—An MPLS traffic engineering tunnel used to protect other (primary) tunnel's traffic when a link or node failure occurs.

**egress router**—A router at the edge of the network where packets are leaving.

**Fast Reroute**—Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**interface**—A network connection.

**IP address**—A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

**IP explicit path**—A list of IP addresses, each representing a node or link in the explicit path.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**link**—Point-to-point connection between adjacent nodes.

**LSP**—label switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**node**—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

**penultimate router**—The second-to-last router; that is, the router that is immediately before the egress router.

**primary tunnel**—An MPLS tunnel whose LSP can be fast rerouted if there is a failure.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**router ID**—Something by which a router originating a packet can be uniquely distinguished from all other routers. For example, an IP address from one of the router's interfaces.

**scalability**—An indicator showing how quickly some measure of resource usage increases as a network gets larger.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**tunnel**—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering—AutoTunnel Mesh Groups

---

**First Published: January 27, 2004**

**Last Updated: October 21, 2009**

The MPLS Traffic Engineering—AutoTunnel Mesh Groups feature allows a network administrator to configure traffic engineering (TE) label switched paths (LSPs) by using a few command-line interface (CLI) commands.

In a network topology where edge TE label switch routers (LSRs) are connected by core LSRs, the MPLS Traffic Engineering—AutoTunnel Mesh Groups feature automatically constructs a mesh of TE LSPs among the provider edge (PE) routers.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering—AutoTunnel Mesh Groups” section on page 18](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—AutoTunnel Mesh Groups, page 2](#)
- [Restrictions for MPLS Traffic Engineering—AutoTunnel Mesh Groups, page 2](#)
- [Information About MPLS Traffic Engineering—AutoTunnel Mesh Groups, page 2](#)
- [How to Configure MPLS Traffic Engineering—AutoTunnel Mesh Groups, page 4](#)
- [Configuration Examples for MPLS Traffic Engineering—Autotunnel Mesh Groups, page 14](#)



---

**Americas Headquarters:**

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

- [Additional References, page 16](#)
- [Feature Information for MPLS Traffic Engineering—AutoTunnel Mesh Groups, page 18](#)
- [Glossary, page 19](#)

## Prerequisites for MPLS Traffic Engineering—AutoTunnel Mesh Groups

- Be knowledgeable about MPLS TE. See the [“Additional References” section on page 16](#).
- Decide how you will set up autotunnels (that is, identify the tunnel commands that you will include in the template interface).
- Identify a block of addresses that you will reserve for mesh tunnel interfaces.

## Restrictions for MPLS Traffic Engineering—AutoTunnel Mesh Groups

- Mesh groups do not support interarea tunnels because the destinations of those tunnels do not exist in the local area TE database.
- You cannot configure a static route to route traffic over autotunnel mesh group TE tunnels. You should use only the autoroute for tunnel selection.
- Intermediate System-to-System (IS-IS) does not support Interior Gateway Protocol (IGP) distribution of mesh group information. For IS-IS, only Access Control Lists (ACLs) can be used.

## Information About MPLS Traffic Engineering—AutoTunnel Mesh Groups

To configure autotunnel mesh groups, you need to understand the following concepts:

- [AutoTunnel Mesh Groups Description and Benefits, page 2](#)
- [Access Lists for Mesh Tunnel Interfaces, page 3](#)
- [AutoTunnel Template Interfaces, page 3](#)
- [OSPF Flooding of Mesh Group Information, page 4](#)

## AutoTunnel Mesh Groups Description and Benefits

An autotunnel mesh group (referred to as a mesh group) is a set of connections between edge LSRs in a network. There are two types of mesh groups:

- Full—All the edge LSRs are connected. Each PE router has a tunnel to each of the other PE routers.
- Partial—Some of the edge LSRs are not connected to each other by tunnels.

In a network topology where edge TE LSRs are connected by core LSRs, the MPLS Traffic Engineering—AutoTunnel Mesh Groups feature automatically constructs a mesh of TE LSPs among the PE routers.

Initially, you must configure each existing TE LSR to be a member of the mesh by using a minimal set of configuration commands. When the network grows (that is, when one or more TE LSRs are added to the network as PE routers), you do not need to reconfigure the existing TE LSR members of that mesh.

Mesh groups have the following benefits:

- Minimize the initial configuration of the network. You configure one template interface per mesh, and it propagates to all mesh tunnel interfaces, as needed.
- Minimize future configurations resulting from network growth. The feature eliminates the need to reconfigure each existing TE LSR to establish a full mesh of TE LSPs whenever a new PE router is added to the network.
- Enable existing routers to configure TE LSPs to new PE routers.
- Enable the construction of a mesh of TE LSPs among the PE routers automatically.

## Access Lists for Mesh Tunnel Interfaces

The access list determines the destination addresses for the mesh tunnel interfaces. It is useful if you preallocate a block of related IP addresses. You can use that block of addresses to control the PE routers to which a full or partial mesh of TE tunnel LSPs is established. The access list allows matches for only the addresses that are learned and stored in the TE topology database.

For example, you can create an access list that matches all 10.1.1.1 IP addresses. You configure a template with the access list, then the template creates mesh tunnel interfaces to destinations within the TE topology database that match destinations in that access list.

Whenever the TE topology database is updated (for example, when a new TE LSR is inserted into the Interior Gateway Protocol (IGP), the destination address is stored in the TE topology database of each router in the IGP. At each update, the Mesh Group feature compares the destination address contained in the database to IP addresses in the access list associated with all template interfaces. If there is a match, the Mesh Group feature establishes a mesh tunnel interface to the tunnel destination IP address.

## AutoTunnel Template Interfaces

An autotunnel template interface is a logical entity; that is, it is a configuration for a tunnel interface that is not tied to specific tunnel interfaces. It can be applied dynamically, when needed.

Mesh tunnel interfaces are tunnel interfaces that are created, configured dynamically (for example, by the applying [or cloning] of a template interface), used, and then freed when they are no longer needed.

A mesh tunnel interface obtains its configuration information from a template, except for the tunnel's destination address, which it obtains from the TE topology database that matches an access list or from the IGP mesh group advertisement.

The template interface allows you to enter commands once per mesh group. These commands specify how mesh tunnel interfaces are created. Each time a new router is added to the network, a new mesh tunnel interface is created. The configuration of the interface is duplicated from the template. Each mesh tunnel interface has the same path constraints and other parameters configured on the template interface. Only the tunnel destination address is different.

## OSPF Flooding of Mesh Group Information

For OSPF to advertise or flood mesh group information, you need to configure a mesh group in OSPF and add that mesh group to an autotemplate interface. When the configuration is complete, OSPF advertises the mesh group IDs to all LSRs. MPLS TE LSPs automatically connect the edge LSRs in each mesh group. For configuration information, see the [“Configuring IGP Flooding for Autotunnel Mesh Groups” section on page 13](#).

OSPF can advertise mesh group IDs for an OSPF area. OSPF is the only IGP supported in the Cisco IOS 12.0(29)S, 12.2(33)SRA, 12.2(33)SXH, and 12.4(20)T releases of the MPLS Traffic Engineering—AutoTunnel Mesh Groups feature.

## How to Configure MPLS Traffic Engineering—AutoTunnel Mesh Groups

This section contains the following procedures:

- [Configuring a Mesh of TE Tunnel LSPs, page 4](#) (required)
- [Specifying the Range of Mesh Tunnel Interface Numbers, page 9](#) (optional)
- [Displaying Configuration Information About Tunnels, page 10](#) (optional)
- [Monitoring the Autotunnel Mesh Network, page 11](#) (required)
- [Configuring IGP Flooding for Autotunnel Mesh Groups, page 13](#) (optional)

## Configuring a Mesh of TE Tunnel LSPs

Perform the following tasks on each PE router in your network to configure a mesh of TE tunnel LSPs:

- [Enabling Autotunnel Mesh Groups Globally, page 4](#)
- [Creating an Access List Using a Name, page 5](#)
- [Creating an Autotunnel Template Interface, page 7](#)

**Note**

You can perform these tasks in any order.

## Enabling Autotunnel Mesh Groups Globally

Perform the following task to enable autotunnel mesh groups globally. Perform this task on all PE routers in your network that you want to be part of an autotunnel mesh group.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel mesh**
4. **end**



## DETAILED STEPS

|        | Command or Action                                                                 | Purpose                                                                                                           |
|--------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                                 |                                                                                                                   |
| Step 2 | <code>configure terminal</code>                                                   | Enters global configuration mode.                                                                                 |
|        | <b>Example:</b><br><code>Router# configure terminal</code>                        |                                                                                                                   |
| Step 3 | <code>mpls traffic-eng auto-tunnel mesh</code>                                    | Enables autotunnel mesh groups globally.                                                                          |
|        | <b>Example:</b><br><code>Router(config)# mpls traffic-eng auto-tunnel mesh</code> |                                                                                                                   |
| Step 4 | <code>end</code>                                                                  | Exits to privileged EXEC mode.                                                                                    |
|        | <b>Example:</b><br><code>Router(config)# end</code>                               |                                                                                                                   |

## Creating an Access List Using a Name

Perform the following task to create an access list using a name.

The access list determines the destination addresses for the mesh tunnel interfaces. You can use an access list to control the PE routers to which a full or partial mesh of TE tunnel LSPs is established. The access list allows matches for only the addresses that are learned and stored in the TE topology database.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip access-list {standard / extended} access-list-name`
4. `permit source [source-wildcard]`
5. `end`

## DETAILED STEPS

|        | Command or Action                                 | Purpose                                                                                                           |
|--------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br><code>Router&gt; enable</code> |                                                                                                                   |

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 3 | <code>ip access-list {standard   extended} access-list-name</code><br><br><b>Example:</b><br>Router(config)# <code>ip access-list standard a1</code> | Defines an IP access list using a name and enters standard named access list configuration mode. <ul style="list-style-type: none"> <li>The <b>standard</b> keyword specifies a standard IP access list.</li> <li>The <b>extended</b> keyword specifies an extended IP access list.</li> <li>The <i>access-list-name</i> argument is the name of the access list. A name cannot contain a space or quotation mark and must begin with an alphabetic character. This prevents confusion with numbered access lists.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 4 | <code>permit source [source-wildcard]</code><br><br><b>Example:</b><br>Router(config-std-nacl)# <code>permit 10.0.0.0 0.255.255.255</code>           | Sets conditions to allow a packet to pass a named IP access list. <ul style="list-style-type: none"> <li>The <i>source</i> argument is the number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: <ul style="list-style-type: none"> <li>Use a 32-bit quantity in four-part dotted decimal format.</li> <li>Use the <b>any</b> keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.</li> <li>Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.</li> </ul> </li> <li>The <i>source-wildcard</i> argument is the wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: <ul style="list-style-type: none"> <li>Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore.</li> <li>Use the <b>any</b> keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255.</li> <li>Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.</li> </ul> </li> </ul> |
| Step 5 | <code>end</code><br><br><b>Example:</b><br>Router(config-std-nacl)# <code>end</code>                                                                 | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Creating an Autotunnel Template Interface

Perform the following task to create an autotunnel template interface. This helps minimize the initial configuration of the network. You configure one template interface per mesh, and it propagates to all mesh tunnel interfaces, as needed.



### Note

You can use the following commands to create a minimal configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface auto-template** *interface-num*
4. **ip unnumbered** *interface-type interface-number*
5. **tunnel mode** {aurp | cayman | dvmrp | eon | gre | ipip | iptalk | mpls | nos}
6. **tunnel mpls traffic-eng autoroute announce**
7. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
8. **tunnel mpls traffic-eng auto-bw** [*collect-bw*] [*frequency seconds*] [*max-bw kbps*] [*min-bw kbps*]
9. **tunnel mpls traffic-eng path-option** *number* {dynamic | explicit {name *path-name* | *path-number*}} [*lockdown*]
10. **tunnel destination access-list** *num*
11. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface auto-template</b> <i>interface-num</i><br><br><b>Example:</b><br>Router(config)# interface auto-template 1           | Creates a template interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>interface-num</i> argument is the interface number. Valid values are from 1 to 25.</li> </ul>                                                                                                                       |
| Step 4 | <b>ip unnumbered</b> <i>interface-type interface-number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered Loopback 0 | Enables IP processing on an interface without assigning an explicit IP address to the interface. <ul style="list-style-type: none"> <li>The <i>type</i> and <i>number</i> arguments name the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.</li> </ul> |

|        | Command or Action                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>tunnel mode {aurp   cayman   dvmrp   eon   gre   ipip   iptalk   mpls   nos}</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mode mpls</p>                                    | Sets the encapsulation mode for the tunnel interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 6 | <pre>tunnel mpls traffic-eng autoroute announce</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>autoroute announce</p>                                        | Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first algorithm (SPF) calculation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | <pre>tunnel mpls traffic-eng priority setup-priority [hold-priority]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>priority 1 1</p>                         | <p>Configures the setup and reservation priority for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>setup-priority</i> argument is the priority used when an LSP is signaled for this tunnel and determines 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.</li> <li>The <i>hold-priority</i> argument is the priority associated with an LSP for this tunnel and determines if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority.</li> </ul>                                                                                                                                                                                                                                                 |
| Step 8 | <pre>tunnel mpls traffic-eng auto-bw [collect-bw] [frequency seconds] [max-bw kbps] [min-bw kbps]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>auto-bw</p> | <p>Configures a tunnel for automatic bandwidth adjustment and for control of the manner in which the bandwidth for a tunnel is adjusted.</p> <ul style="list-style-type: none"> <li>The <b>collect-bw</b> keyword collects output rate information for the tunnel, but does not adjust the tunnel's bandwidth.</li> <li>The <b>frequency seconds</b> keyword-argument pair is the interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. Do not specify a value lower than the output rate sampling interval specified in the <b>mpls traffic-eng auto-bw</b> command in global configuration mode.</li> <li>The <b>max-bw kbps</b> keyword-argument pair is the maximum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.</li> <li>The <b>min-bw kbps</b> keyword-argument pair is the minimum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.</li> </ul> |

|         | Command or Action                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <pre>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number}} [lockdown]</pre> <p><b>Example:</b></p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic</pre> | <p>Configures a path option for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument is the number of the path option. When multiple path options are configured, lower numbered options are preferred.</li> <li>The <b>dynamic</b> keyword specifies that the path of the LSP is dynamically calculated.</li> <li>The <b>explicit</b> keyword specifies that the path of the LSP is an IP explicit path.</li> <li>The <b>name path-name</b> keyword-argument pair is the path name of the IP explicit path that the tunnel uses with this option.</li> <li>The <i>path-number</i> argument is the path number of the IP explicit path that the tunnel uses with this option.</li> <li>The <b>lockdown</b> keyword specifies that the LSP cannot be reoptimized.</li> </ul> |
| Step 10 | <pre>tunnel destination access-list num</pre> <p><b>Example:</b></p> <pre>Router(config-if)# tunnel destination access-list 1</pre>                                                                                     | <p>Specifies the access list that the template interface uses for obtaining the mesh tunnel interface destination address.</p> <ul style="list-style-type: none"> <li>The <i>num</i> argument is the number of the access list.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 11 | <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end</pre>                                                                                                                                                    | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Specifying the Range of Mesh Tunnel Interface Numbers

Perform the following task to specify the range of mesh tunnel interface numbers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel mesh tunnel-num min *num* max *num***
4. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <b>mpls traffic-eng auto-tunnel mesh tunnel-num min num max num</b><br><br><b>Example:</b><br>Router(config)# <b>mpls traffic-eng auto-tunnel mesh tunnel-num min 1000 max 2000</b> | Specifies the range of mesh tunnel interface numbers. <ul style="list-style-type: none"> <li>The <b>min num</b> keyword-argument pair specifies the beginning number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535.</li> <li>The <b>max num</b> keyword-argument pair specifies the ending number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535.</li> </ul> |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                                                                     | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                  |

## Displaying Configuration Information About Tunnels

Perform the following task to display tunnel configuration information, such as tunnel interface and mesh tunnel configuration.

## SUMMARY STEPS

- enable**
- show running interface auto-template num**
- show interface tunnel num configuration**
- exit**

## DETAILED STEPS

|        |                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br>Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:<br>Router> <b>enable</b><br>Router#                                                              |
| Step 2 | <b>show running interface auto-template num</b><br><br>Use this command to display interface configuration information for a tunnel interface. For example:<br>Router# <b>show running interface auto-template 1</b> |

```
interface auto-templ1
 ip unnumbered Loopback0
 no ip directed-broadcast
 no keepalive
 tunnel destination access-list 1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
```

This output shows that autotunnel template interface auto-templ1 uses an access list (access-list 1) to determine the destination addresses for the mesh tunnel interfaces.

**Step 3** **show interface tunnel *num* configuration**

Use this command to display the configuration of the mesh tunnel interface. For example:

```
Router# show interface tunnel 5 configuration
```

```
interface tunnel 5
 ip unnumbered Loopback0
 no ip directed-broadcast
 no keepalive
 tunnel destination access-list 1
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 1 dynamic
```

**Step 4** **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

---

## Monitoring the Autotunnel Mesh Network

Perform the following task to monitor the autotunnel mesh network.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels property auto-tunnel mesh [brief]**
3. **show mpls traffic-eng auto-tunnel mesh**
4. **exit**

### DETAILED STEPS

---

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng tunnels property auto-tunnel mesh [brief]**

Use this command to monitor mesh tunnel interfaces. This command restricts the output of the **show mpls traffic-eng tunnels** command to display only mesh tunnel interfaces. For example:

```
Router# show mpls traffic-eng tunnels property auto-tunnel mesh brief

Signalling Summary:
LSP Tunnels Process:      running
RSVP Process:             running
Forwarding:               enabled
Periodic reoptimization:  every 3600 seconds, next in 491 seconds
Periodic FRR Promotion:   Not Running
Periodic auto-bw collection: disabled
TUNNEL NAME               DESTINATION    UP IF    DOWN IF
STATE/PROT
router_t64336              10.2.2.2      -        Se2/0
up/up
router_t64337              10.3.3.3      -        Se2/0
up/up
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

### Step 3 **show mpls traffic-eng auto-tunnel mesh**

Use this command to display the cloned mesh tunnel interfaces of each autotemplate interface and the current range of mesh tunnel interface numbers. For example:

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

Auto-Templatel:

Using access-list 1 to clone the following tunnel interfaces:

Destination  Interface
-----
10.2.2.2     Tunnel64336
10.3.3.3     Tunnel64337

Mesh tunnel interface numbers: min 64336 max 65337
```

### Step 4 **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Troubleshooting Tips

You can configure mesh tunnel interfaces directly. However, you cannot delete them manually, and manual configuration is not permanent. The configuration is overwritten when the template changes or the mesh tunnel interface is deleted and re-created. If you attempt to manually delete a mesh tunnel interface, an error message appears.

You can enter the **show mpls traffic-eng tunnels destination *address*** command to display information about tunnels that are destined for a specified IP address.

Enter the **show mpls traffic-eng tunnels property auto-tunnel mesh** command to display information about mesh tunnel interfaces.



## Configuring IGP Flooding for Autotunnel Mesh Groups

Perform the following task to configure IGP flooding for autotunnel mesh groups. Use this task to configure an OSPF-based discovery for identifying mesh group members and advertising the mesh group IDs to all LSRs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel mesh**
4. **router ospf** *process-id*
5. **mpls traffic-eng mesh-group** *mesh-group-id* *interface-type* *interface-number* **area** *area-id*
6. **exit**
7. Repeat steps 4 and 5 at other LSRs to advertise the mesh group numbers to which they belong.
8. **interface auto-template** *interface-num*
9. **tunnel destination mesh-group** *mesh-group-id*
10. **end**

### DETAILED STEPS

|        | Command or Action                                                    | Purpose                                                                              |
|--------|----------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                        | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable                                    | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                                            | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal                        |                                                                                      |
| Step 3 | <b>mpls traffic-eng auto-tunnel mesh</b>                             | Enables autotunnel mesh groups globally.                                             |
|        | <b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel mesh |                                                                                      |

|         | Command or Action                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <b>router</b> <i>ospf process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 100                                                                                                           | Enters router configuration mode and configures an OSPF routing process. <ul style="list-style-type: none"> <li>The <i>process-id</i> argument is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.</li> </ul>                                        |
| Step 5  | <b>mpls traffic-eng mesh-group</b> <i>mesh-group-id interface-type interface-number area area-id</i><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng mesh-group 10 loopback 0 area 100 | Advertises the autotunnel mesh group number of an LSR. <ul style="list-style-type: none"> <li>The <i>mesh-group-id</i> is a number that identifies a specific mesh group.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments specify a type of interface and an interface number.</li> <li>The <b>area area-id</b> keyword-argument pair identifies the area.</li> </ul> |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                                                        | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                            |
| Step 7  | Repeat steps 4 and 5 at other LSRs to advertise the mesh group numbers to which they belong.                                                                                                             | —                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 8  | <b>interface auto-template</b> <i>interface-num</i><br><br><b>Example:</b><br>Router(config)# interface auto-template 1                                                                                  | Creates a template interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>interface-num</i> argument identifies the interface number. Valid values are from 1 to 25.</li> </ul>                                                                                                                                                                      |
| Step 9  | <b>tunnel destination mesh-group</b> <i>mesh-group-id</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination mesh-group 10                                                                  | Specifies a mesh group that a template interface uses to signal tunnels for all mesh group members. <ul style="list-style-type: none"> <li>The <i>mesh-group-id</i> is a number that identifies a specific mesh group.</li> </ul>                                                                                                                                                              |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                 |

## Configuration Examples for MPLS Traffic Engineering—Autotunnel Mesh Groups

This section contains the following configuration examples:

- [Configuring a Mesh of TE Tunnel LSPs: Examples, page 15](#)
- [Specifying the Range of Mesh Tunnel Interface Numbers: Example, page 16](#)
- [Configuring IGP Flooding for Autotunnel Mesh Groups: Example, page 16](#)

## Configuring a Mesh of TE Tunnel LSPs: Examples

This section contains the following configuration examples for configuring a mesh of TE tunnel LSP:

- [Enabling Autotunnel Mesh Groups Globally: Example, page 15](#)
- [Creating an Access List Using a Name: Example, page 15](#)
- [Creating an AutoTunnel Template Interface: Example, page 15](#)

### Enabling Autotunnel Mesh Groups Globally: Example

The following example shows how to enable autotunnel mesh groups globally:

```
configure terminal
!

mpls traffic-eng auto-tunnel mesh
end
```

### Creating an Access List Using a Name: Example

The following examples shows how to create an access list using a name to determine the destination addresses for the mesh tunnel interfaces:

```
configure terminal
!
ip access-list standard a1
 permit 10.0.0.0 0.255.255.255
end
```

In this example, any IP address in the TE topology database that matches access list a1 causes the creation of a mesh tunnel interface with that destination address.

### Creating an AutoTunnel Template Interface: Example

This example shows how to create an AutoTunnel template template interface. In the following example, an AutoTunnel template is created and configured with a typical set of TE commands. The mesh group created from the template consists of mesh tunnel interfaces with destination addresses that match access list a1.

**Note**

---

The following example shows a typical configuration.

---

```
configure terminal
!
interface auto-template 1
 ip unnumbered Loopback0
 tunnel mode mpls
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng auto-bw
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel destination access-list a1
end
```

## Specifying the Range of Mesh Tunnel Interface Numbers: Example

In the following example, the lowest mesh tunnel interface number can be 1000, and the highest mesh tunnel interface number can be 2000:

```
configure terminal
!
mpls traffic-eng auto-tunnel mesh tunnel-num min 1000 max 2000
end
```

## Configuring IGP Flooding for Autotunnel Mesh Groups: Example

In the following example, OSPF is configured to advertise the router membership in mesh group 10:

```
configure terminal
!
mpls traffic-eng auto-tunnel mesh
router ospf 100
 mpls traffic-eng mesh-group 10 loopback 0 area 100
exit
!
interface auto-template 1
 tunnel destination mesh-group 10
end
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—AutoTunnel Mesh Groups feature.

## Related Documents

| Related Topic                                 | Document Title                                                            |
|-----------------------------------------------|---------------------------------------------------------------------------|
| MPLS traffic engineering command descriptions | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for MPLS Traffic Engineering—AutoTunnel Mesh Groups

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering—AutoTunnel Mesh Groups

| Feature Name                                    | Releases                                                                         | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—AutoTunnel Mesh Groups | 12.0(27)S<br>12.0(29)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T<br>12.2(33)SRE | <p>The MPLS Traffic Engineering—AutoTunnel Mesh Groups feature allows a network administrator to configure TE LSPs.</p> <p>In Cisco IOS Release 12.2(27)S, this feature was introduced.</p> <p>In Cisco IOS Release 12.0(29)S, this feature was updated to include Interior Gateway Protocol (IGP) flooding of autotunnel mesh groups.</p> <p>In Cisco IOS Release 12.2(33)SRA, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SXH, support was added.</p> <p>In Cisco IOS Release 12.4(20)T, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was integrated. A router with autotunnel mesh groups can be configured with stateful switchover (SSO) redundancy.</p> |

# Glossary

**CE router**—customer edge router. A router that is part of a customer's network and interfaces to a provider edge (PE) router.

**customer network**—A network that is under the control of an end customer. Private addresses can be used in a customer network. Customer networks are logically isolated from each other and from the service provider's network.

**edge router**—A router at the edge of the network that receives and transmits packets. It can define the boundaries of the Multiprotocol Label Switching (MPLS) network.

**headend**—The label switch router (LSR) where a tunnel originates. The tunnel's "head" or tunnel interface resides at this LSR as well.

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets).

**label switched path (LSP) tunnel**—A configured connection between two routers in which label switching is used to carry the packets.

**LSP**—label switched path. A path that a labeled packet follows over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**mesh group**—A set of label switch routers (LSRs) that are members of a full or partial network of traffic engineering (TE) label switched paths (LSPs).

**P router**—provider core router.

**PE router**—provider edge router. A router at the edge of the service provider's network that interfaces to customer edge (CE) routers.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**tailend**—The downstream, receive end of a tunnel.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**tunnel**—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing.

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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering—Verbatim Path Support

---

**First Published: August 26, 2003**

**Last Updated: February 27, 2008**

The MPLS Traffic Engineering—Verbatim Path Support feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for traffic engineering (TE), thereby bypassing the topology database verification process.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering—Verbatim Path Support”](#) section on [page 9](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—Verbatim Path Support, page 2](#)
- [Restrictions for MPLS Traffic Engineering—Verbatim Path Support, page 2](#)
- [Information About MPLS Traffic Engineering—Verbatim Path Support, page 2](#)
- [How to Configure and Verify MPLS Traffic Engineering—Verbatim Path Support, page 2](#)
- [Configuration Example for MPLS Traffic Engineering—Verbatim Path Support, page 7](#)
- [Additional References, page 7](#)



---

**Americas Headquarters:**

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

- [Command Reference, page 8](#)
- [Glossary, page 10](#)

## Prerequisites for MPLS Traffic Engineering—Verbatim Path Support

- An MPLS TE tunnel must be configured globally.
- MPLS TE must be enabled on all links.

## Restrictions for MPLS Traffic Engineering—Verbatim Path Support

- The **verbatim** keyword can be used only on a label-switched path (LSP) that is configured with the explicit path option.
- This release does not support reoptimization on the verbatim LSP.
- You cannot configure MPLS Traffic Engineering over the logical GRE tunnel interface.

## Information About MPLS Traffic Engineering—Verbatim Path Support

MPLS TE LSPs usually require that all the nodes in the network are TE aware, meaning they have IGP extensions to TE in place. However, some network administrators want the ability to build TE LSPs to traverse nodes that do not support IGP extensions to TE, but that do support RSVP extensions to TE.

Verbatim LSPs are helpful when all or some of the intermediate nodes in a network do not support IGP extensions for TE.

When this feature is enabled, the IP explicit path is not checked against the TE topology database. Because the TE topology database is not verified, a Path message with IP explicit path information is routed using the shortest path first (SPF) algorithm for IP routing.

## How to Configure and Verify MPLS Traffic Engineering—Verbatim Path Support

This section contains the following procedures:

- [Configuring MPLS Traffic Engineering—Verbatim Path Support, page 3](#) (required)
- [Verifying Verbatim LSPs for MPLS TE Tunnels, page 6](#) (optional)

# Configuring MPLS Traffic Engineering—Verbatim Path Support

Perform this task to configure MPLS traffic engineering—verbatim path support.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered loopback** *number*
5. **tunnel destination** {*host-name* | *ip-address*}
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** {**sub-pool** *kbps* | *kbps*}
8. **tunnel mpls traffic-eng autoroute announce**
9. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
10. **tunnel mpls traffic-eng path-option** *preference-number* {**dynamic** [*attributes string* | **bandwidth** {**sub-pool** *kbps* | *kbps*} | **lockdown** | **verbatim**} | **explicit** {**name** *path-name* | **identifier** *path-number*}}
- or -
- tunnel mpls traffic-eng path-option protect** *preference-number* {**dynamic** [*attributes string* | **bandwidth** {**sub-pool** *kbps* | *kbps*} | **explicit** {**name** *path-name* | **identifier** *path-number*} | *attributes string* | **bandwidth** {**sub-pool** *kbps* | *kbps*} | **verbatim**}]}
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                 | Purpose                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                |
| Step 3 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                | Enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>number</i> argument identifies the tunnel number to be configured.</li> </ul>                                                                                                                                 |
| Step 4 | <b>ip unnumbered loopback</b> <i>number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 1 | Configures an unnumbered IP interface, which enables IP processing without an explicit address. A loopback interface is usually configured with the router ID.<br><br><b>Note</b> An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |

|        | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>tunnel destination</b> { <i>host-name</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.100.100.100                        | Specifies the destination for a tunnel. <ul style="list-style-type: none"> <li>The <i>host-name</i> argument is the name of the host destination.</li> <li>The <i>ip-address</i> argument is the IP Version 4 address of the host destination expressed in decimal in four-part, dotted notation.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                            | Sets the tunnel encapsulation mode to MPLS traffic engineering.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>tunnel mpls traffic-eng bandwidth</b> { <i>sub-pool kbps</i>   <i>kbps</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng bandwidth 1000      | Configures the bandwidth required for an MPLS TE tunnel and assigns it either to the sub-pool or the global pool. <ul style="list-style-type: none"> <li>The <b>sub-pool</b> keyword indicates a subpool tunnel.</li> <li>The <i>kbps</i> argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Step 8 | <b>tunnel mpls traffic-eng autoroute announce</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng autoroute announce                                | Specifies that IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 9 | <b>tunnel mpls traffic-eng priority</b> <i>setup-priority</i> [ <i>hold-priority</i> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng priority 1 1 | Configures setup and reservation priority for a tunnel. <ul style="list-style-type: none"> <li>The <i>setup-priority</i> argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted.<br/><br/>Valid values are from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.</li> <li>The <i>hold-priority</i> argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled.<br/><br/>Valid values are from 0 to 7, where a lower number indicates a higher priority.</li> </ul> |

|         | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <pre> <b>tunnel mpls traffic-eng path-option</b>   <i>preference-number</i> {<b>dynamic</b> [<b>attributes</b> <i>string</i>   <b>bandwidth</b> {<b>sub-pool</b> <i>kbps</i>   <i>kbps</i>}   <b>lockdown</b>   <b>verbatim</b>]   <b>explicit</b> {<b>name</b> <i>path-name</i>   <b>identifier</b> <i>path-number</i>}} - or - <b>tunnel mpls traffic-eng path-option protect</b>   <i>preference-number</i> {<b>dynamic</b> [<b>attributes</b> <i>string</i>   <b>bandwidth</b> {<b>sub-pool</b> <i>kbps</i>   <i>kbps</i>}]   <b>explicit</b> {<b>name</b> <i>path-name</i>   <b>identifier</b> <i>path-number</i>} [<b>attributes</b> <i>string</i>   <b>bandwidth</b> {<b>sub-pool</b> <i>kbps</i>   <i>kbps</i>}   <b>verbatim</b>]}  <b>Example:</b> Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test verbatim  Router(config-if)# tunnel mpls traffic-eng path-option protect 2 dynamic name test 2 bandwidth sub-pool 34 </pre> | <p>Specifies LSP-related parameters, including the <b>verbatim</b> keyword used with an explicit path option, for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> <li>The <i>preference-number</i> argument identifies the path option.</li> <li>The <b>protect</b> keyword and <i>preference-number</i> argument identify the path option with protection.</li> <li>The <b>dynamic</b> keyword indicates that the path option is dynamically calculated. (The router figures out the best path.)</li> <li>The <b>explicit</b> keyword indicates that the path option is specified. The IP addresses are specified for the path.</li> <li>The <b>name</b> <i>path-name</i> keyword argument combination identifies the name of the explicit path option.</li> <li>The <i>path-number</i> argument identifies the number of the explicit path option.</li> <li>The <b>verbatim</b> keyword bypasses the topology database verification.</li> </ul> <p><b>Note</b> You can use the <b>verbatim</b> keyword only with the explicit path option.</p> <ul style="list-style-type: none"> <li>The <b>attributes</b> <i>string</i> keyword argument combination names an attribute list to specify path options for the LSP.</li> <li>The <b>bandwidth</b> keyword specifies the LSP bandwidth.</li> <li>The <b>sub-pool</b> keyword indicates a subpool path option.</li> <li>The <i>kbps</i> argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.</li> <li>The <b>lockdown</b> keyword disables reoptimization of the LSP.</li> </ul> |
| Step 11 | <pre> <b>end</b>  <b>Example:</b> Router(config)# end </pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Verifying Verbatim LSPs for MPLS TE Tunnels

Perform this task to verify that the verbatim option is configured for the LSPs for MPLS TE tunnels.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels *tunnel-interface* [brief]**
3. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                            | Purpose                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show mpls traffic-eng tunnels <i>tunnel-interface</i> [brief]</b><br><br><b>Example:</b><br>Router# show mpls traffic-eng tunnels tunnel1 | Displays information about tunnels including those configured with an explicit path option using verbatim.            |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                     | (Optional) Exits to user EXEC mode.                                                                                   |

### Examples

In the following example, the **show mpls traffic-eng tunnels** command displays tunnel information, including whether the explicit path option is using verbatim and the Active Path Options Parameters that show the status of verbatim.

```
Router# show mpls traffic-eng tunnels tunnel100

Name: GSR-2_t100                               (Tunnel100) Destination: 192.168.30.1
Status:
  Admin: up           Oper: up           Path: valid           Signalling: connected

  path option 1, type explicit (verbatim) BACKUP (Basis for Setup, path weight 0)

Config Parameters:
  Bandwidth: 0          kbps (Global)  Priority: 7 7    Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: disabled  LockDown: disabled  Loadshare: 0      bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: enabled
```

# Configuration Example for MPLS Traffic Engineering—Verbatim Path Support

This section provides the following configuration example:

- [Configuring MPLS Traffic Engineering—Verbatim Path Support, page 7](#)

## Configuring MPLS Traffic Engineering—Verbatim Path Support

The following example shows a tunnel that has been configured with an explicit path option using verbatim:

```
interface tunnel 1
 ip unnumbered loopback 1
 tunnel destination 10.10.100.100
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 explicit name path1 verbatim
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—Verbatim Path feature.

## Related Documents

| Related Topic                    | Document Title                                                        |
|----------------------------------|-----------------------------------------------------------------------|
| MPLS Label Distribution Protocol | <a href="#">MPLS Label Distribution Protocol (LDP) feature module</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                    | Title |
|--------------------------------------------------------|-------|
| No new or modified RFCs are supported by this release. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **show mpls traffic-eng tunnels**
- **tunnel mpls traffic-eng path option**



# Feature Information for MPLS Traffic Engineering—Verbatim Path Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering—Verbatim Path Support

| Feature Name                                   | Releases                                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—Verbatim Path Support | 12.0(26)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS Traffic Engineering—Verbatim Path Support feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for traffic engineering (TE), thereby bypassing the topology database verification process.</p> <p>In 12.0(26)S, this feature was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRA.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> <p>The following commands were introduced or modified:<br/><b>show mpls traffic-eng tunnels, tunnel mpls traffic-eng path option.</b></p> |

# Glossary

**Fast Reroute**—Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the head end.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

**LSP**—label-switched path. A configured connection between two routers, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

**LSR**—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**merge point**—The backup tunnel's tail.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**PLR**—point of local repair. The head-end of the backup tunnel.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

**SPF**—shortest path first. Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**tunnel**—A secure communications path between two peers, such as routers.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2003, 2006, 2008 Cisco Systems, Inc. All rights reserved.



# MPLS Traffic Engineering—RSVP Hello State Timer

---

**First Published: August 2, 2004**  
**Last Updated: February 27, 2009**

The MPLS Traffic Engineering—RSVP Hello State Timer feature detects when a neighbor is down and quickly triggers a state timeout, which frees resources such as bandwidth that can be reused by other label switched paths (LSPs).

RSVP hellos can be used to detect when a neighboring node is down. The hello state timer then triggers a state timeout. As a result, network convergence time is reduced, and nodes can forward traffic on alternate paths or assist in stateful switchover (SSO) operation.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS Traffic Engineering—RSVP Hello State Timer](#)” section on page 13.

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—RSVP Hello State Timer](#), page 2
- [Restrictions for MPLS Traffic Engineering—RSVP Hello State Timer](#), page 2
- [Information About MPLS Traffic Engineering—RSVP Hello State Timer](#), page 2
- [How to Configure MPLS Traffic Engineering—RSVP Hello State Timer](#), page 5
- [Configuration Examples for MPLS Traffic Engineering—RSVP Hello State Timer](#), page 10



---

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

- [Additional References, page 11](#)
- [Command Reference, page 12](#)

## Prerequisites for MPLS Traffic Engineering—RSVP Hello State Timer

Perform the following tasks on routers before configuring the MPLS Traffic Engineering—RSVP Hello State Timer feature:

- Configure Resource Reservation Protocol (RSVP).
- Enable Multiprotocol Label Switching (MPLS).
- Configure traffic engineering (TE).
- Enable hellos for state timeout.

## Restrictions for MPLS Traffic Engineering—RSVP Hello State Timer

- Hellos for state timeout are dependent on graceful restart, if it is configured; however, graceful restart is independent of hellos for state timeout.
- Unnumbered interfaces are not supported.
- Hellos for state timeout are configured on a per-interface basis.

## Information About MPLS Traffic Engineering—RSVP Hello State Timer

You should understand the following concepts before configuring the MPLS TE—RSVP Hello State Timer feature:

- [Hellos for State Timeout, page 2](#)

### Hellos for State Timeout

When RSVP signals a TE LSP and there is a failure somewhere along the path, the failure can remain undetected for as long as two minutes. During this time, bandwidth is held by the nonfunctioning LSP on the nodes downstream from the point of failure along the path with the state intact. If this bandwidth is needed by headend tunnels to signal or resignal LSPs, tunnels may fail to come up for several minutes thereby negatively affecting convergence time.

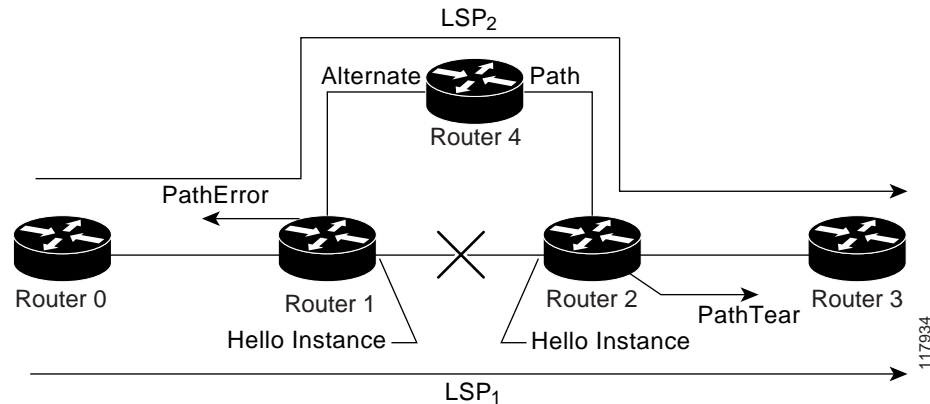
Hellos enable RSVP nodes to detect when a neighboring node is not reachable. After a certain number of intervals, hellos notice that a neighbor is not responding and delete its state. This action frees the node's resources to be reused by other LSPs.

Hellos must be configured both globally on the router and on the specific interface to be operational.

## Nonfast-Reroutable TE LSP

Figure 1 shows a nonfast-reroutable TE LSP from Router 1 to Router 3 via Router 2.

**Figure 1** *Nonfast-Reroutable TE LSP*



Assume that the link between Router 1 and Router 2 fails. This type of problem can be detected by various means including interface failure, Interior Gateway Protocol (IGP) (Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS)), and RSVP hellos. However, sometimes interface failure cannot be detected; for example, when Router 1 and Router 2 are interconnected through a Layer 2 switch. The IGP may be slow detecting the failure. Or there may be no IGP running between Router 1 and Router 2; for example, between two Autonomous System Boundary Routers (ASBRs) interconnecting two autonomous systems.

If hellos were running between Router 1 and Router 2, each router would notice that communication was lost and time out the state immediately.

Router 2 sends a delayed PathTear message to Router 3 so that the state can be deleted on all nodes thereby speeding up the convergence time.



### Note

The PathTear message is delayed one second because on some platforms data is being forwarded even after the control plane is down.

Router 1 sends a destructive PathError message upstream to Router 0 with error code ROUTING\_PROBLEM and error value NO\_ROUTE.

LSP1 goes from Router 0 to Router 1 to Router 2 to Router 3; LSP 2 goes from Router 0 to Router 1 to Router 4 to Router 2 to Router 3.

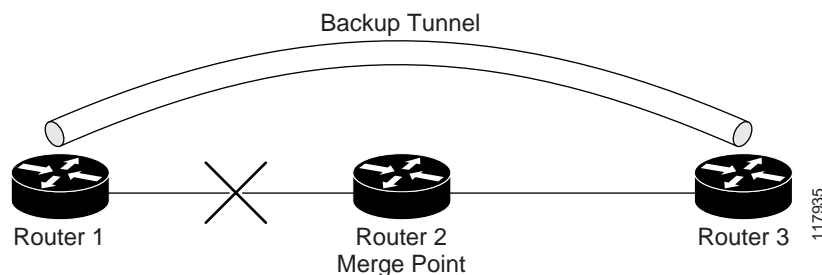
## Hello Instance

A hello instance implements RSVP hellos for a given router interface address and a remote IP address. A hello instance is expensive because of the large number of hello requests that are sent and the strains they put on the router resources. Therefore, you should create a hello instance only when it is needed to time out state and delete the hello instance when it is no longer necessary.

## Fast-Reroutable TE LSP with Backup Tunnel

Figure 2 shows a fast reroutable TE LSP with a backup tunnel from Router 1 to Router 2 to Router 3.

**Figure 2** *Fast Reroutable TE LSP with Backup Tunnel*



This TE LSP has a backup tunnel from Router 1 to Router 3 protecting the fast reroutable TE LSP against a failure in the Router 1 to Router 2 link and node Router 2. However, assume that a failure occurs in the link connecting Router 1 to Router 2. If hellos were running between Router 1 and Router 2, the routers would notice that the link is down, but would not time out the state. Router 2 notices the failure, but cannot time out the TE LSP because Router 2 may be a merge point, or another downstream node may be a merge point. Router 1 notices the failure and switches to the backup LSP; however, Router 1 cannot time out the state either.



### Note

A hello instance is not created in the preceding scenario because the neighbor is down and the hello instance cannot take action.

## Fast-Reroutable TE LSP Without Backup Tunnel

On a fast-reroutable TE LSP with no backup tunnel, a hello instance can be created with the neighbor downstream (next hop (NHOP)). On a nonfast-reroutable TE LSP, a hello instance can be created with the neighbor downstream (NHOP) and the neighbor upstream (previous hop (PHOP)). This is in addition to the existing hellos for Fast Reroute.

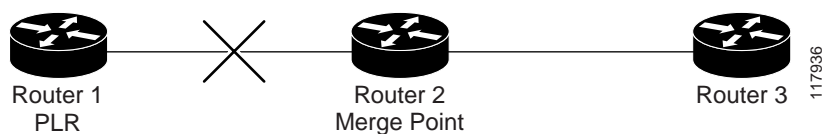


### Note

If both Fast Reroute and hellos for state timeout hello instances are needed on the same link, only one hello instance is created. It will have the Fast Reroute configuration including interval, missed refreshes, and differentiated services code point (DSCP). When a neighbor is down, Fast Reroute and the hello state timer take action.

Figure 3 shows a fast-reroutable TE LSP, without a backup tunnel, from Router 1 (the point of local repair (PLR)), to Router 2 to Router 3.

**Figure 3** *Fast Reroutable TE LSP Without Backup Tunnel*



Assume that a failure occurs in the link connecting Router 1 to Router 3. Router 1 can time out the state for the TE LSP because Router 1 knows there is no backup tunnel. However, Router 2 cannot time out the state because Router 2 does not know whether a backup tunnel exists. Also, Router 2 may be a merge point, and therefore cannot time out the state.

**Note**

A hello instance is not created in the preceding scenario because the neighbor is down and the hello instance cannot take action.

## How to Configure MPLS Traffic Engineering—RSVP Hello State Timer

This section contains the following procedures:

**Note**

The following tasks also enable Fast Reroute; however, this section focuses on the RSVP hello state timer.

- [Enabling the Hello State Timer Globally, page 5](#) (required)
- [Enabling the Hello State Timer on an Interface, page 6](#) (required)
- [Setting a DSCP Value on an Interface, page 7](#) (optional)
- [Setting a Hello Request Interval on an Interface, page 8](#) (optional)
- [Setting the Number of Hello Messages that can be Missed on an Interface, page 9](#) (optional)
- [Verifying Hello for State Timer Configuration, page 10](#) (optional)

### Enabling the Hello State Timer Globally

Perform this task to enable the RSVP hello state timer globally to reduce network convergence, allow nodes to forward traffic on alternate paths, or assist in stateful switchover (SSO) operation.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello**
4. **end**

## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip rsvp signalling hello</b><br><br><b>Example:</b><br>Router(config)# ip rsvp signalling hello | Enables hellos for state timeout globally on a router.                                                           |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                           | Exits to privileged EXEC mode.                                                                                   |

## Enabling the Hello State Timer on an Interface

Perform this task to enable the RSVP hello state timer on an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp signalling hello**
5. **end**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |



|        | Command or Action                                                                                     | Purpose                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/0  | Enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type number</i> arguments identify the interface to be configured.</li> </ul> |
| Step 4 | <b>ip rsvp signalling hello</b><br><br><b>Example:</b><br>Router(config-if)# ip rsvp signalling hello | Enables hellos for state timeout on an interface.                                                                                                                |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                           | Exits to privileged EXEC mode.                                                                                                                                   |

## Setting a DSCP Value on an Interface

Perform this task to set a differentiated services code point DSCP value for hello messages on an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp signalling hello reroute dscp** *num*
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                    | Purpose                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                       | Enters global configuration mode.                                                                                                                                |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/0 | Enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type number</i> arguments identify the interface to be configured.</li> </ul> |

|        | Command or Action                                                                                                                                                                | Purpose                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>ip</b> <b>rsvp</b> <b>signalling</b> <b>hello</b> <b>reroute</b> <b>dscp</b> <i>num</i><br><br><b>Example:</b><br>Router(config-if)# ip rsvp signalling hello reroute dscp 30 | Sets a DSCP value for RSVP hello messages on an interface of a router from 0 to 63 with hellos for state timeout enabled. |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                                      | Exits to privileged EXEC mode.                                                                                            |

## Setting a Hello Request Interval on an Interface

Perform this task to set a hello request interval on an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp signalling hello reroute refresh interval** *interval-value*
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                    | Purpose                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                       | Enters global configuration mode.                                                                                                                                   |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/0 | Enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type number</i> argument identifies the interface to be configured.</li> </ul> |

|        | Command or Action                                                                                                                                                                | Purpose                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Step 4 | <pre>ip rsvp signalling hello reroute refresh interval interval-value</pre> <p><b>Example:</b><br/>Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000</p> | Sets a hello request interval on an interface of a router with hellos for state timer enabled. |
| Step 5 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                 | Exits to privileged EXEC mode.                                                                 |

## Setting the Number of Hello Messages that can be Missed on an Interface

Perform this task to set the number of consecutive hello messages that are lost (missed) before hello declares the neighbor down.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type number**
4. **ip rsvp signalling hello reroute refresh misses msg-count**
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                 |
| Step 2 | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p>                | Enters global configuration mode.                                                                                                                                  |
| Step 3 | <pre>interface type number</pre> <p><b>Example:</b><br/>Router(config)# interface Ethernet 0/0</p> | Enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type number</i> arguments identify the interface to be configured.</li> </ul> |

|        | Command or Action                                                                                                                                                           | Purpose                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Step 4 | <pre>ip rsvp signalling hello reroute refresh misses msg-count</pre> <p><b>Example:</b></p> <pre>Router(config-if)# ip rsvp signalling hello reroute refresh misses 5</pre> | Configures the number of consecutive hello messages that are lost before hello declares the neighbor down. |
| Step 5 | <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config-if)# end</pre>                                                                                                     | Exits to privileged EXEC mode.                                                                             |

## Verifying Hello for State Timer Configuration

Perform this task to verify the hello for state timer configuration.

### SUMMARY STEPS

1. `enable`
2. `show ip rsvp hello`

### DETAILED STEPS

|        | Command or Action                                                                          | Purpose                                                                                                                       |
|--------|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b></p> <pre>Router&gt; enable</pre>                      | (Optional) Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <pre>show ip rsvp hello</pre> <p><b>Example:</b></p> <pre>Router# show ip rsvp hello</pre> | Displays the status of RSVP TE hellos and statistics including hello state timer (reroute).                                   |

## Configuration Examples for MPLS Traffic Engineering—RSVP Hello State Timer

This section provides a configuration example for the MPLS TE—RSVP Hello State Timer feature:

- [MPLS Traffic Engineering—RSVP Hello State Timer: Example, page 10](#)

### MPLS Traffic Engineering—RSVP Hello State Timer: Example

In the following example, the hello state timer is enabled globally and on an interface. Related parameters, including a DSCP value, a refresh interval, and a missed refresh limit, are set on an interface.

```
Router# configure terminal
```

```

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling hello
Router(config)# interface Ethernet 0/0
Router(config-if)# ip rsvp signalling hello
Router(config-if)# ip rsvp signalling hello reroute dscp 30
Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000
Router(config-if)# ip rsvp signalling hello reroute refresh misses 5
Router(config-if)# end

```

The following example verifies the status of the hello state timer (reroute):

```

Router# show ip rsvp hello

Hello:
  Fast-Reroute/Reroute:Enabled
  Statistics:Enabled
  Graceful Restart:Enabled (help-neighbor only)

```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—RSVP Hello State Timer feature.

## Related Documents

| Related Topic                                                                                  | Document Title                                                                                                          |
|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>                                                |
| QoS features including signaling, classification, and congestion management                    | <a href="#">Cisco IOS Quality of Service Solutions Configuration Guide</a>                                              |
| Stateful Switchover                                                                            | <a href="#">Cisco IOS High Availability Configuration Guide</a>                                                         |
| MPLS Label Distribution Protocol                                                               | <a href="#">MPLS Label Distribution Protocol (LDP) Overview</a>                                                         |
| Cisco nonstop forwarding                                                                       | <a href="#">Cisco Nonstop Forwarding</a>                                                                                |
| Information on backup tunnels, link and node failures, RSVP hellos                             | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a> |
| Graceful restart                                                                               | <a href="#">NSF/SSO - MPLS TE and RSVP Graceful Restart</a>                                                             |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                              |
|----------|--------------------------------------------------------------------|
| RFC 3209 | <a href="#"><i>RSVP-TE: Extensions to RSVP for LSP Tunnels</i></a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **ip rsvp signalling hello dscp**
- **ip rsvp signalling hello refresh interval**
- **ip rsvp signalling hello refresh misses**
- **ip rsvp signalling hello reroute dscp**
- **ip rsvp signalling hello reroute refresh interval**
- **ip rsvp signalling hello reroute refresh misses**

- `show ip rsvp hello`

## Feature Information for MPLS Traffic Engineering—RSVP Hello State Timer

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering—RSVP Hello State Timer

| Feature Name                                    | Releases                                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—RSVP Hello State Timer | 12.0(29)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS Traffic Engineering—RSVP Hello State Timer feature detects when a neighbor is down and quickly triggers a state timeout, which frees resources such as bandwidth that can be reused by other label switched paths (LSPs).</p> <p>In 12.0(29)S, this feature was introduced.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRA.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> |

# Glossary

**autonomous system**—A collection of networks that share the same routing protocol and that are under the same system administration.

**ASBR**—autonomous system boundary router. A router that connects and exchanges information between two or more autonomous systems.

**backup tunnel**—An MPLS traffic engineering tunnel used to protect other (primary) tunnel traffic when a link or node failure occurs.

**DSCP**—differentiated services code point. Six bits in the IP header, as defined by the IETF. These bits determine the class of service provided to the IP packet.

**Fast Reroute**—A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**graceful restart**—A process for helping a neighboring Route Processor restart after a node failure has occurred.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

**IS-IS**—Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol whereby Intermediate System (IS) routers exchange routing information based on a single metric to determine network topology.

**instance**—A mechanism that implements the RSVP hello extensions for a given router interface address and remote IP address. Active hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**label**—A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

**LDP**—Label Distribution Protocol. The protocol that supports MPLS hop-by-hop forwarding by distributing bindings between labels and network prefixes. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label switched path is a configured connection between two routers, in which MPLS is used to carry packets. The LSP is created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded by swapping labels from one MPLS node to another MPLS node.

**merge point**—The backup tunnel's tail.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. MPLS enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

**OSPF**—Open Shortest Path First. A link-state routing protocol used for routing.

**PLR**—point of local repair. The headend of the backup tunnel.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.



**state**—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**topology**—The physical arrangement of network nodes and media within an enterprise networking structure.

**tunnel**—Secure communications path between two peers, such as two routers.

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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering Forwarding Adjacency

---

**First Published: January 29, 2001**

**Last Updated: February 27, 2009**

The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a traffic engineering (TE) label switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm.

Both Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) are supported.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering Forwarding Adjacency” section on page 11](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering Forwarding Adjacency, page 2](#)
- [Restrictions for MPLS Traffic Engineering Forwarding Adjacency, page 2](#)
- [Information About MPLS Traffic Engineering Forwarding Adjacency, page 2](#)
- [How to Configure MPLS Traffic Engineering Forwarding Adjacency, page 3](#)
- [Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 10](#)



---

**Americas Headquarters:**

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

- [Feature Information for MPLS Traffic Engineering Forwarding Adjacency, page 11](#)
- [Glossary, page 12](#)

## Prerequisites for MPLS Traffic Engineering Forwarding Adjacency

Your network must support the following Cisco IOS features:

- Multiprotocol Label Switching (MPLS)
- IP Cisco Express Forwarding
- IS-IS

## Restrictions for MPLS Traffic Engineering Forwarding Adjacency

- Using the MPLS Traffic Engineering Forwarding Adjacency feature increases the size of the IGP database by advertising a TE tunnel as a link.
- When the MPLS Traffic Engineering Forwarding Adjacency feature is enabled on a TE tunnel, the link is advertised in the IGP network as a type, length, value (TLV) 22 object without any TE sub-TLV.
- You must configure MPLS TE forwarding adjacency tunnels bidirectionally.
- You cannot configure MPLS Traffic Engineering over the logical GRE tunnel interface.

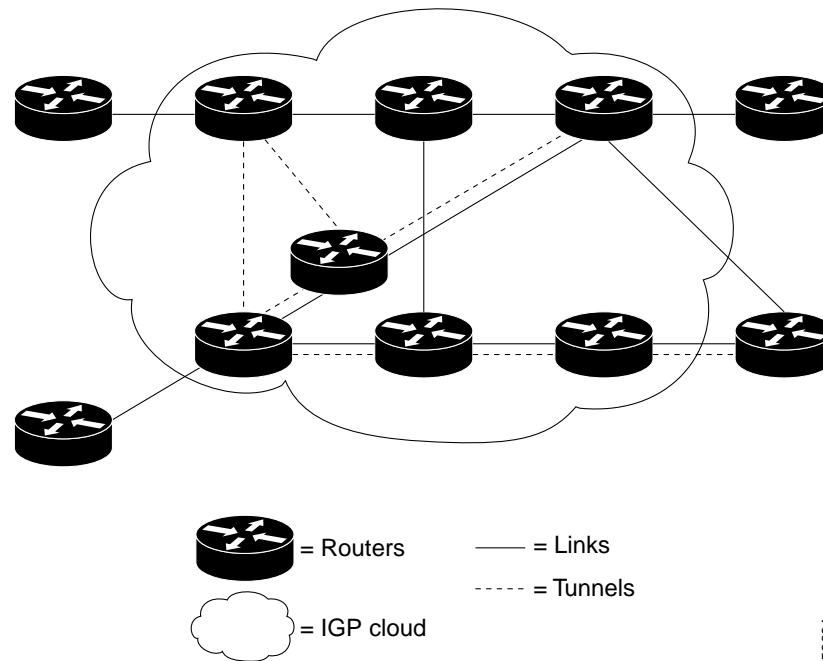
## Information About MPLS Traffic Engineering Forwarding Adjacency

To configure MPLS Traffic Engineering Forwarding Adjacency you should understand the following concepts:

- [MPLS Traffic Engineering Forwarding Adjacency Functionality, page 2](#)
- [MPLS Traffic Engineering Forwarding Adjacency Benefits, page 3](#)

## MPLS Traffic Engineering Forwarding Adjacency Functionality

The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a TE LSP tunnel as a link in an IGP network based on the SPF algorithm. A forwarding adjacency can be created between routers regardless of their location in the network. The routers can be located multiple hops from each other, as shown in [Figure 1](#).

**Figure 1 Forwarding Adjacency Topology**

As a result, a TE tunnel is advertised as a link in an IGP network with the link's cost associated with it. Routers outside of the TE domain see the TE tunnel and use it to compute the shortest path for routing traffic throughout the network.

## MPLS Traffic Engineering Forwarding Adjacency Benefits

### TE Tunnel Interfaces Advertised for SPF

TE tunnel interfaces are advertised in the IGP network just like any other links. Routers can then use these advertisements in their IGP's to compute the SPF even if they are not the headend of any TE tunnels.

## How to Configure MPLS Traffic Engineering Forwarding Adjacency

This section contains the following tasks:

- [Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency, page 3](#) (required)
- [Configuring MPLS TE Forwarding Adjacency on Tunnels, page 4](#) (required)
- [Verifying MPLS TE Forwarding Adjacency, page 5](#) (optional)

## Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency

To configure a tunnel interface for an MPLS TE forwarding adjacency, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***

## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                  |
| Step 3 | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 0 | Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode.               |

## Configuring MPLS TE Forwarding Adjacency on Tunnels

To configure an MPLS TE forwarding adjacency, perform the following steps.

**Note**

You must configure a forwarding adjacency on two LSP tunnels bidirectionally, from A to B and B to A. Otherwise, the forwarding adjacency is advertised, but not used in the IGP network.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **tunnel mpls traffic-eng forwarding-adjacency [holdtime *value*]**
5. **isis metric {*metric-value* | maximum} {level-1 | level-2}**

## DETAILED STEPS

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>interface tunnel number</b><br><br><b>Example:</b><br>Router(config)# interface tunnel 0                                                                    | Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode.                                                                                                                                                                                                                                                         |
| Step 4 | <b>tunnel mpls traffic-eng forwarding-adjacency [holdtime value]</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency | Advertises a TE tunnel as a link in an IGP network.                                                                                                                                                                                                                                                                                                          |
| Step 5 | <b>isis metric {metric-value   maximum} {level-1   level-2}</b><br><br><b>Example:</b><br>Router(config-if)# isis metric 2 level-1                             | Configures the IS-IS metric for a tunnel interface to be used as a forwarding adjacency. <ul style="list-style-type: none"> <li>You should specify the <b>isis metric</b> command with level-1 or level-2 to be consistent with the IGP level at which you are performing traffic engineering. Otherwise, the metric has the default value of 10.</li> </ul> |

## Verifying MPLS TE Forwarding Adjacency

To verify MPLS TE forwarding adjacency on tunnels, perform the following steps.

## SUMMARY STEPS

- show mpls traffic-eng forwarding-adjacency [ip-address]**
- show isis [process-tag] database [level-1] [level-2] [11] [12] [detail] [lspid]**

## DETAILED STEPS

**Step 1** **show mpls traffic-eng forwarding-adjacency [ip-address]**

Use this command to see the current tunnels.

Router# **show mpls traffic-eng forwarding-adjacency**

```
destination 0168.0001.0007.00 has 1 tunnels
Tunnel7      (traffic share 100000, nexthop 192.168.1.7)
              (flags:Announce Forward-Adjacency, holdtime 0)
```

```
Router# show mpls traffic-eng forwarding-adjacency 192.168.1.7

destination 0168.0001.0007.00 has 1 tunnels
Tunnel7      (traffic share 100000, nexthop 192.168.1.7)
              (flags:Announce Forward-Adjacency, holdtime 0)
```

## Step 2 show isis [process-tag] database [level-1] [level-2] [l1] [l2] [detail] [lspid]

Use this command to display information about the IS-IS link-state database.

```
Router# show isis database
```

IS-IS Level-1 Link State Database

| LSPID                | LSP Seq Num | LSP Checksum | LSP Holdtime | ATT/P/OL |
|----------------------|-------------|--------------|--------------|----------|
| 0000.0C00.0C35.00-00 | 0x0000000C  | 0x5696       | 792          | 0/0/0    |
| 0000.0C00.40AF.00-00 | 0x00000009  | 0x8452       | 1077         | 1/0/0    |
| 0000.0C00.62E6.00-00 | 0x0000000A  | 0x38E7       | 383          | 0/0/0    |
| 0000.0C00.62E6.03-00 | 0x00000006  | 0x82BC       | 384          | 0/0/0    |
| 0800.2B16.24EA.00-00 | 0x00001D9F  | 0x8864       | 1188         | 1/0/0    |
| 0800.2B16.24EA.01-00 | 0x00001E36  | 0x0935       | 1198         | 1/0/0    |

IS-IS Level-2 Link State Database

| LSPID                | LSP Seq Num | LSP Checksum | LSP Holdtime | ATT/P/OL |
|----------------------|-------------|--------------|--------------|----------|
| 0000.0C00.0C35.03-00 | 0x00000005  | 0x04C8       | 792          | 0/0/0    |
| 0000.0C00.3E51.00-00 | 0x00000007  | 0xAF96       | 758          | 0/0/0    |
| 0000.0C00.40AF.00-00 | 0x0000000A  | 0x3AA9       | 1077         | 0/0/0    |

# Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency

This section provides the following configuration example for the MPLS Traffic Engineering Forwarding Adjacency feature using an IS-IS metric: [MPLS Traffic Engineering Forwarding Adjacency](#)

## MPLS TE Forwarding Adjacency: Example

The following output shows the configuration of a tunnel interface, a forwarding adjacency, and an IS-IS metric:

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# interface tunnel 7
Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency
Router(config-if)# isis metric 2 level-1
```

Following is sample command output when a forwarding adjacency has been configured:

```
Router# show running-config
```

```
Building configuration...
Current configuration :364 bytes
!
interface Tunnel7
```



```

ip unnumbered Loopback0
no ip directed-broadcast
tunnel destination 192.168.1.7
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng forwarding-adjacency
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng path-option 10 explicit name short
isis metric 2 level 1

```

**Note**

Do not specify the **tunnel mpls traffic-eng autoroute announce** command in your configuration when you are using forwarding adjacency.

Following is an example where forwarding adjacency is configured with OSPF:

```
Router# configure terminal
```

```
Router# show running-config
```

```

Building configuration...
Current configuration : 310 bytes
interface tunnel 1
!
interface Tunnell
 ip unnumbered Loopback0
 ip ospf cost 6
 tunnel destination 172.16.255.5
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency tunnel mpls
 traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
 end

```

```
Router# show mpls traffic-eng forwarding-adjacency
```

```

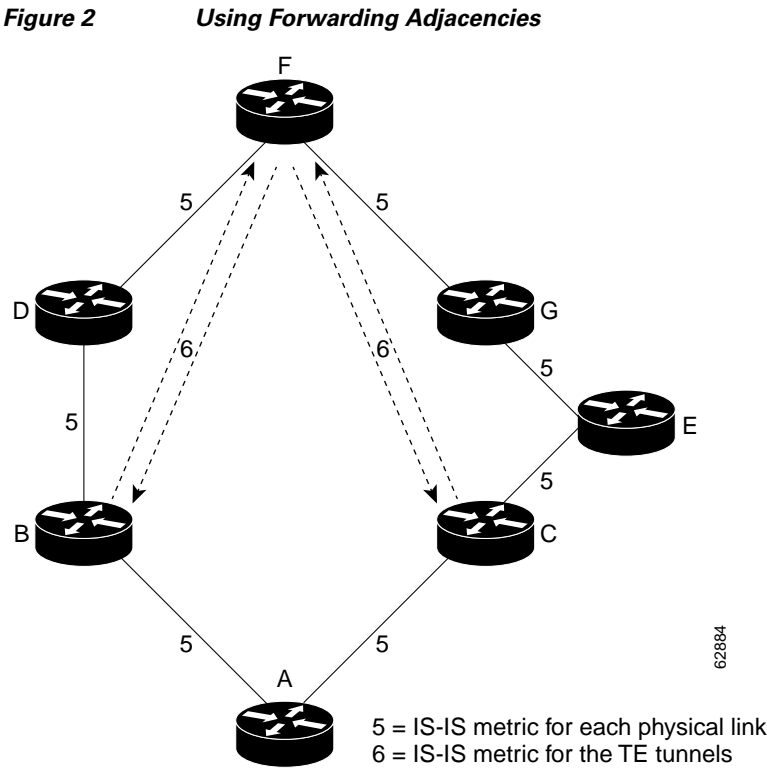
destination 172.16.255.5, area ospf 172 area 0, has 1 tunnels
  Tunnell      (load balancing metric 2000000, nexthop 172.16.255.5)
                (flags: Forward-Adjacency, holdtime 0)

```

```
Router#
```

## Usage Tips

In [Figure 2](#), if you have no forwarding adjacencies configured for the TE tunnels between Band F and C and F, all the traffic that A must forward to F goes through B because B is the shortest path from A to F. (The cost from A to F is 15 through B and 20 through C.)



If you have forwarding adjacencies configured on the TE tunnels between B and F and C and F and also on the TE tunnels between F and B and F and C, then when A computes the SPF algorithm, A sees two equal cost paths of 11 to F. As a result, traffic across the A-B and A-C links is shared.

62884

# Additional References

The following sections provide references related to the MPLS Traffic Engineering Forwarding Adjacency feature.

## Related Documents

| Related Topic                     | Document Title                                                                        |
|-----------------------------------|---------------------------------------------------------------------------------------|
| MPLS traffic engineering commands | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>             |
| Switching services commands       | <a href="#">Cisco IOS IP Switching Command Reference</a>                              |
| IS-IS TLVs                        | <a href="#">Intermediate System-to-Intermediate System (IS-IS) TLVs</a> (white paper) |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                              | MIBs Link                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing standards has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **debug mpls traffic-eng forwarding-adjacency**
- **show mpls traffic-eng forwarding-adjacency**
- **tunnel mpls traffic-eng forwarding-adjacency**

# Feature Information for MPLS Traffic Engineering Forwarding Adjacency

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering Forwarding Adjacency

| Feature Name                                  | Releases                                                                                      | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering Forwarding Adjacency | 12.0(15)S<br>12.0(16)ST<br>12.2(18)S<br>12.2(18)SXD<br>12.2(27)SBC<br>12.2(28)SB<br>12.4(20)T | The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a TE LSP tunnel as a link in an IGP network based on the SPF algorithm.<br><br>In 12.0(15)S, this feature was introduced.<br>In 12.0(16)ST, this feature was integrated.<br>In 12.2(18)S, this feature was integrated.<br>In 12.2(18)SXD, this feature was integrated.<br>In 12.2(27)SBC, this feature was integrated.<br>In 12.2(28)SB, this feature was integrated.<br>In 12.4(20)T, this feature was integrated. The following commands were modified: <b>debug mpls traffic-eng forwarding-adjacency</b> , <b>show mpls traffic-eng forwarding-adjacency</b> , and <b>tunnel mpls traffic-eng forwarding-adjacency</b> . |

# Glossary

**Cisco Express Forwarding**—A scalable, distributed, Layer 3 switching solution designed to meet the future performance requirements of the Internet and enterprise networks.

**forwarding adjacency**—A traffic engineering link (or LSP) into an IS-IS/OSPF network.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**IS-IS**—Intermediate System-to-Intermediate System. Open System Interconnection (OSI) link-state hierarchical routing protocol whereby Intermediate System (IS) routers exchange routing information based on a single metric to determine network topology.

**label switched path (LSP)**—A sequence of hops ( $R_0 \dots R_n$ ) in which a packet travels from  $R_0$  to  $R_n$  through label switching mechanisms. A switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**label switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**OSPF**—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol. *See also* IS-IS.

**SPF**—Shortest Path First. A routing algorithm used as the basis for OSPF operations. When an SPF router is powered up, it initializes its routing-protocol data structures and then waits for indications from lower-layer protocols that its interfaces are functional.

**TLV**—type, length, value. A block of information embedded in Cisco Discovery Protocol advertisements.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been applied.

**traffic engineering tunnel**—A label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing would cause the tunnel to take.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2001–2009 Cisco Systems, Inc. All rights reserved.







# MPLS Traffic Engineering : Class-based Tunnel Selection

---

**First Published: November 1, 2003**

**Last Updated: May 9, 2008**

The MPLS Traffic Engineering (TE): Class-based Tunnel Selection feature enables you to dynamically route and forward traffic with different class of service (CoS) values onto different TE tunnels between the same tunnel headend and the same tailend. The TE tunnels can be regular TE or DiffServ-aware TE (DS-TE) tunnels.

The set of TE (or DS-TE) tunnels from the same headend to the same tailend that you configure to carry different CoS values is referred to as a “tunnel bundle.” After configuration, Class-Based Tunnel Selection (CBTS) dynamically routes and forwards each packet into the tunnel that:

- Is configured to carry the CoS of the packet
- Has the right headend for the destination of the packet

Because CBTS offers dynamic routing over DS-TE tunnels and requires minimum configuration, it greatly eases deployment of DS-TE in large-scale networks.

CBTS can distribute all CoS values on eight different tunnels.

CBTS also allows the TE tunnels of a tunnel bundle to exit headend routers through different interfaces.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS Traffic Engineering : Class-based Tunnel Selection](#)” section on page 30.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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



---

**Americas Headquarters:**

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

© 2003–2008 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for MPLS Traffic Engineering : Class-based Tunnel Selection, page 2](#)
- [Restrictions for MPLS Traffic Engineering : Class-based Tunnel Selection, page 2](#)
- [Information About MPLS Traffic Engineering : Class-based Tunnel Selection, page 2](#)
- [How to Configure MPLS Traffic Engineering : Class-based Tunnel Selection, page 10](#)
- [Configuration Examples for MPLS Traffic Engineering : Class-based Tunnel Selection, page 19](#)
- [Additional References, page 28](#)
- [Command Reference, page 29](#)
- [Feature Information for MPLS Traffic Engineering : Class-based Tunnel Selection, page 30](#)
- [Glossary, page 31](#)

## Prerequisites for MPLS Traffic Engineering : Class-based Tunnel Selection

- Multiprotocol Label Switching (MPLS) must be enabled on all tunnel interfaces.
- Cisco Express Forwarding or distributed Cisco Express Forwarding must be enabled in global configuration mode.

## Restrictions for MPLS Traffic Engineering : Class-based Tunnel Selection

- For a given destination, all CoS values are carried in tunnels terminating at the same tailend. Either all CoS values are carried in tunnels or no values are carried in tunnels. In other words, for a given destination, you cannot map some CoS values in a DS-TE tunnel and other CoS values in a Shortest Path First (SPF) Label Distribution Protocol (LDP) or SPF IP path.
- CBTS does not allow load-balancing of a given experimental (EXP) value in multiple tunnels. If two or more tunnels are configured to carry a given EXP value, CBTS picks one of those tunnels to carry this EXP value.
- The operation of CBTS is not supported with Any Transport over MPLS (AToM), MPLS TE Automesh, or label-controlled (LC)-ATM.

## Information About MPLS Traffic Engineering : Class-based Tunnel Selection

To configure the MPLS Traffic Engineering (TE): Class-based Tunnel Selection feature, you should understand the following concepts:

- [Incoming Traffic Supported by MPLS TE Class-based Tunnel Selection, page 3](#)
- [CoS Attributes for MPLS TE Class-based Tunnel Selection, page 3](#)

- [Routing Protocols and MPLS TE Class-based Tunnel Selection, page 3](#)
- [Tunnel Selection with MPLS TE Class-based Tunnel Selection, page 4](#)
- [DS-TE Tunnels and MPLS TE Class-based Tunnel Selection, page 10](#)
- [Reoptimization and MPLS TE Class-based Tunnel Selection, page 10](#)
- [Interarea and Inter-AS and MPLS TE Class-based Tunnel Selection, page 10](#)
- [ATM PVCs and MPLS TE Class-based Tunnel Selection, page 10](#)

## Incoming Traffic Supported by MPLS TE Class-based Tunnel Selection

The CBTS feature supports the following kinds of incoming packets:

- At a provider edge (PE) router—Unlabeled packets that enter a Virtual Private Network (VPN) routing and forwarding (VRF) instance interface
- At a provider core (P) router—Unlabeled and MPLS-labeled packets that enter a non-VRF interface
- At a PE router in a Carrier Supporting Carrier (CSC) or interautonomous system (Inter-AS)—MPLS-labeled packets that enter a VRF interface

## CoS Attributes for MPLS TE Class-based Tunnel Selection

CBTS supports tunnel selection based on the value of the EXP field that the headend router imposes on the packet. Before imposing this value, the router considers the input modular quality of service (QoS) command-line interface (CLI) (MQC). If the input MQC modifies the EXP field value, CBTS uses the modified value for its tunnel selection.

Packets may enter the headend from multiple incoming interfaces. These interfaces can come from different customers that have different DiffServ policies. In such cases, service providers generally use input MQC to apply their own DiffServ policies and mark imposed EXP values accordingly. Thus, CBTS can operate consistently for all customers by considering the EXP values marked by the service provider.



### Note

---

If the output MQC modifies the EXP field, CBTS ignores the change in the EXP value.

---

CBTS allows up to eight different tunnels on which it can distribute all classes of service.

## Routing Protocols and MPLS TE Class-based Tunnel Selection

CBTS routes and forwards packets to MPLS TE tunnels for specified destinations through use of the following routing protocols:

- Intermediate System-to-Intermediate System (IS-IS) with Autoroute configured
- Open Shortest Path First (OSPF) with Autoroute configured
- Static routing
- Border Gateway Protocol (BGP) with recursion configured on the BGP next hop with packets forwarded on the tunnel through the use of IS-IS, OSPF, or static routing

## Tunnel Selection with MPLS TE Class-based Tunnel Selection

This section contains the following topics related to tunnel selection:

- [EXP Mapping Configuration, page 4](#)
- [Tunnel Selection for EXP Values, page 4](#)
- [Tunnel Failure Handling, page 7](#)
- [Misordering of Packets, page 9](#)

### EXP Mapping Configuration

With CBTS, you can configure each tunnel with any of the following:

- The same EXP information configured as it was before the CBTS feature was introduced, that is, with no EXP-related information
- One or more EXP values for the tunnel to carry
- A property that allows the carrying of all EXP values not currently allocated to any up-tunnel (default)
- One or more EXP values for the tunnel to carry, and the default property that allows the carrying of all EXP values not currently allocated to any up-tunnel

The default property (the carrying of all EXP values not currently allocated to any up-tunnel) effectively provides a way for the operator to avoid explicitly listing all possible EXP values. Even more important, the default property allows the operator to indicate tunnel preferences onto which to “bump” certain EXP values, should the tunnel carrying those EXP values go down. (See the [tunnel mpls traffic-eng exp](#) command for the command syntax.)

The configuration of each tunnel is independent of the configuration of any other tunnel. CBTS does not attempt to perform any consistency check for EXP configuration.

This feature allows configurations where:

- Not all EXP values are explicitly allocated to tunnels.
- Multiple tunnels have the default property.
- Some tunnels have EXP values configured and others do not have any values configured.
- A given EXP value is configured on multiple tunnels.

### Tunnel Selection for EXP Values

This section contains information about the following topics:

- [Tunnel Selection Process, page 5](#)
- [Tunnel Selection Examples, page 5](#)
- [Multipath with Non-TE Paths and MPLS TE Class-Based Tunnel Selection, page 7](#)
- [MPLS TE Class-Based Tunnel Selection and Policy-Based Routing, page 7](#)

## Tunnel Selection Process

Tunnel selection with this feature is a two-step process:

1. For a given prefix, routing (autoroute, static routes) occurs exactly as it did without the CBTS feature. The router selects the set of operating tunnels that have the best metrics, regardless of the EXP-related information configured on the tunnel.
2. CBTS maps all of the EXP values to the selected set of tunnels:
  - If a given EXP value is configured:
    - On only one of the tunnels in the selected set, CBTS maps the EXP value onto that tunnel.
    - On two or more of the tunnels in the selected set, CBTS arbitrarily maps the EXP value onto one of these tunnels. First CBTS selects the tunnel on which the lowest EXP value is explicitly configured. Then CBTS picks the tunnel that has the lowest tunnel ID.
  - If a given EXP value is not configured on any of the tunnels in the selected set:
    - And only one of the tunnels in the selected set is configured as a default, CBTS maps the EXP value onto that tunnel.
    - And two or more of the tunnels in the selected set are configured as defaults, CBTS arbitrarily maps the EXP value onto one of these tunnels.
    - And no tunnel in the selected set of tunnels is configured as a default, CBTS does not map this EXP value onto any specific tunnel. Instead, CBTS performs CoS-unaware load balancing of that EXP information across all tunnels in the selected set.

CBTS relies on autoroute to select the tunnel bundle. Autoroute selects only tunnels that are on the SPF to the destination. Therefore, similar to Autoroute, CBTS does not introduce any risk of routing loops.

## Tunnel Selection Examples

The following examples show various tunnel configurations that are set up by an operator and indicate how CBTS maps packets carrying EXP values onto these tunnels. Each example describes a different configuration: a default tunnel configured, more than one tunnel configured with the same EXP value, and so on.

### Example 1—Default Tunnel Configured

An operator configures the following parameters on tunnels T1 and T2:

- T1: exp = 5, autoroute
- T2: exp = default, autoroute

If T1 and T2 are next-hop interfaces for prefix P, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1
- Packets with <Dest = P, exp = anything-other-than-5> onto T2

### Example 2—EXP Values Configured on Two Tunnels; One Default Tunnel

An operator configures the following parameters on tunnels T1, T2, and T3:

- T1: exp = 5, autoroute
- T2: exp = 3 and 4, autoroute
- T3: exp = default, autoroute

If T1, T2, and T3 are next-hop interfaces for prefix P, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1
- Packets with <Dest = P, exp = 3 or 4> onto T2
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T3

### Example 3—More than One Tunnel with the Same EXP

An operator configures the following parameters on tunnels T1, T2, and T3:

- T1: exp = 5, autoroute
- T2: exp = 5, autoroute
- T3: exp = default, autoroute

If T1, T2, and T3 are next-hop interfaces for prefix P, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1 (arbitrary selection)
- Packets with <Dest = P, exp = anything-other-than-5> onto T3
- No packets onto T2

### Example 4—Static Route Configured

An operator configures the following parameters on tunnels T1 and T2:

- T1: exp = 5, autoroute
- T2: exp = 3
- Static route to P on T2

If prefix P is behind the T1 and T2 tailend router, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = anything> onto T2
- No packets onto T1

Static routes are preferred over dynamic routes; therefore, the router chooses only T2 as the “selected set” of tunnels.

### Example 5—Metrics Configured on Tunnels

An operator configures the following parameters on tunnels T1 and T2:

- T1: exp = 5, autoroute, relative metric –2
- T2: exp = 3, autoroute, relative metric –3

CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = anything> onto T2
- No packets onto T1

The autoroute tunnel selection algorithm selects the tunnel with the best metric. Therefore, the router selects only T2 as the “selected set” of tunnels.

### Example 6—No Default or Metric Configuration

An operator configures the following parameters on tunnels T1 and T2:

- T1: exp = 5, autoroute
- T2: exp = 3, autoroute

If T1 and T2 are the next-hop interfaces for prefix P, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1
- Packets with <Dest = P, exp = 3> onto T2
- Packets with <Dest = P, exp = anything-other-than-3-or-5> onto T2

If a packet arrives with an EXP value that is different from any value configured for a tunnel, the packet goes in to the default tunnel. If no default tunnel is configured, the packet goes in to the tunnel that is configured with the lowest EXP value.

## Multipath with Non-TE Paths and MPLS TE Class-Based Tunnel Selection

For a given prefix in the routing process, the router might select a set of paths that includes both TE tunnels and non-TE-tunnel paths (SPF paths). For example, internal Border Gateway Protocol (iBGP) Multipath might be activated and result in multiple BGP next hops for that prefix, where one BGP next hop is reachable through TE tunnels and other BGP next hops are reachable through non-TE-tunnel paths.

An equal cost IGP path might also exist over TE tunnels and over a non-TE tunnel path. For example, a TE tunnel metric might be modified to be equal to the SPF path.

In these situations, CBTS maps traffic in the following manner:

- If a given EXP value is configured on one or more of the tunnels in the selected set, CBTS maps the EXP value onto that tunnel or one of those tunnels.
- If a given EXP value is not configured on any of the tunnels in the selected set but one or more of the tunnels is configured as a default in the selected set, then CBTS maps the EXP value onto that tunnel or one of those tunnels.
- If a given EXP value is not configured on any of the tunnels from the selected set and no tunnel in the selected set is configured as a default, CBTS performs CoS-unaware load-balancing of that EXP value across all the possible paths, including all of the TE tunnels of the selected set and the non-TE paths.
- If the routing process allocates all EXP values to tunnels or if a default is used, then routing does not use the non-TE paths unless all TE tunnels are down.

## MPLS TE Class-Based Tunnel Selection and Policy-Based Routing

If you configure both policy-based routing (PBR) over TE tunnels (in non-VRF environments) and CBTS, the PBR decision overrides the CBTS decision. PBR is an input process that the router performs ahead of regular forwarding.

## Tunnel Failure Handling

This section contains the following sections:

- [Tunnel Up or Down, page 7](#)
- [Behavior When a Tunnel Goes Down, page 8](#)

### Tunnel Up or Down

For CBTS operation, the important question is whether the tunnel interface is up or down, not whether the current TE label switched path (LSP) is up or down. For example, a TE LSP might go down but is reestablished by the headend because another path option exists. The tunnel interface does not go down during the transient period while the TE LSP is reestablished. Because the tunnel interface does not go down, the corresponding EXP does not get rerouted onto another tunnel during the transient period.

## Behavior When a Tunnel Goes Down

When a tunnel used by CBTS for forwarding goes down, the feature adjusts its tunnel selection for the affected EXP values. It reapplies the tunnel selection algorithm to define the behavior of packets for all EXP values, as shown in the examples that follow.

### Example 1—Tunnel Other than the Default Tunnel Goes Down

An operator configures the following parameters on tunnels T1, T2, and T3:

- T1: exp = 5, autoroute
- T2: exp = 3 and 4, autoroute
- T3: exp = default, autoroute

If T1, T2, and T3 are next-hop interfaces for prefix P and Tunnel T1 goes down, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 3, 4> onto T2 (as before)
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T3 (as before)
- Packets with <Dest = P, exp = 5> onto T3

### Example 2—Default Tunnel Goes Down

An operator configures the following parameters on tunnels T1, T2, and T3:

- T1: exp = 5, autoroute
- T2: exp = 3 and 4, autoroute
- T3: exp = default, autoroute

If T1, T2, and T3 are next-hop interfaces for prefix P and Tunnel T3 goes down, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1 (as before)
- Packets with <Dest = P, exp = 3, 4> onto T2 (as before)
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T1 and T2, following existing CoS-unaware load balancing

### Example 3—Two Default Tunnels Are Configured

An operator configures the following parameters on tunnels T1, T2, and T3:

- T1: exp = 5, autoroute
- T2: exp = 3, 4, and default, autoroute
- T3: exp = 0, 1, 2, 6, 7, and default, autoroute

If T1, T2, and T3 are next-hop interfaces for prefix P and Tunnel T3 goes down, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1 (as before)
- Packets with <Dest = P, exp = 3, 4> onto T2 (as before)
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T2

If tunnel T2 goes down, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 5> onto T1 (as before)
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T3 (as before)



- Packets with <Dest = P, exp = 3, or 4> onto T3

If tunnel T1 goes down, CBTS maps the packets onto the tunnels in this way:

- Packets with <Dest = P, exp = 3, or 4> onto T2 (as before)
- Packets with <Dest = P, exp = 0, 1, 2, 6, or 7> onto T3 (as before)
- Packets with <Dest = P, exp = 5> onto either T2 or T3, but not both

In Example 3, the operator configures the EXP default option on two tunnels to ensure that nonvoice traffic is never redirected onto the voice tunnel (T1).

## Misordering of Packets

In DiffServ, packets from a given flow might get marked with EXP values that are different from each other but belong to the same CoS value because of in-contract and out-of-contract marking of packets. We can refer to these values of EXP bits as EXP-in and EXP-out.

If packets for EXP-in are sent on a different tunnel than packets for EXP-out, then misordering of packets within the same flows could occur. For that reason, CBTS allows operators to ensure that EXP-in and EXP-out never get mapped onto different tunnels.

The CBTS feature allows the operator to configure EXP-in and EXP-out to be transported on the same tunnel when that tunnel is up. This ensures that the feature does not introduce misordering of packets. In case of tunnel failure, the tunnel selection algorithm ensures that if EXP-in and EXP-out were carried on the same tunnel before the failure, they are still carried on a single tunnel after the failure. Thus, CBTS protects against nontransient misordering even in the event of tunnel failure.



**Note**

CBTS does not attempt to force EXP-in and EXP-out to be carried on the same tunnel. The operator must configure CBTS so that EXP-in and EXP-out are carried on the same tunnel. This is comparable to the regular DiffServ situation, where the operator must ensure that EXP-in and EXP-out are configured to go in the same queue.

## Fast Reroute and MPLS TE Class-based Tunnel Selection

CBTS allows Fast Reroute (FRR) protection on tunnels for which you configure CoS-based selection.

CBTS operation with FRR does not change the number of or the way in which FRR backup tunnels might be used. The operation of FRR is the same as when CBTS is not activated. After you configure primary tunnels from a given headend to a given tailend, you can use FRR in the same way whether you activate CoS-based tunnel selection or not. This includes the following possibilities:

- None of the tunnels use FRR.
- All of the  $x$  tunnels are FRR-protected and share the same backup tunnel, if the traffic goes out the same interface.
- Some of the  $x$  tunnels are not FRR-protected; the remaining tunnels are FRR-protected and share the same backup tunnel, if the traffic goes out the same interface.
- Some of the  $x$  tunnels are not FRR-protected; the remaining tunnels are FRR-protected and are protected by different backup tunnels (for example, if the traffic goes out different interfaces, or if the traffic goes out the same interface). Bandwidth guarantees exist on the backup tunnels.

The important question for CBTS operation is only whether a tunnel interface goes down or stays up. FRR protects a given tunnel in exactly the same way as if CBTS were not configured on the tunnel.

## DS-TE Tunnels and MPLS TE Class-based Tunnel Selection

CBTS operates over tunnels using DS-TE. Therefore, the tunnels on which CoS-based selection is performed can each arbitrarily and independently use a bandwidth from the global pool or the subpool.

## Reoptimization and MPLS TE Class-based Tunnel Selection

CBTS allows tunnels on which CoS-based selection is performed to be reoptimized. Reoptimization does not affect CBTS operation.

## Interarea and Inter-AS and MPLS TE Class-based Tunnel Selection

The CBTS operates over tunnels that are interarea when the interarea tunnels use static routes on destination prefixes or on the BGP next hops.

## ATM PVCs and MPLS TE Class-based Tunnel Selection

CBTS operates over ATM permanent virtual circuits (PVCs). This means that TE or DS-TE tunnels handled by CBTS can span links that are ATM PVCs. ATM PVCs might be used on the headend router that is running CBTS and on transit label switch routers (LSRs).

# How to Configure MPLS Traffic Engineering : Class-based Tunnel Selection

This section contains the following procedures:

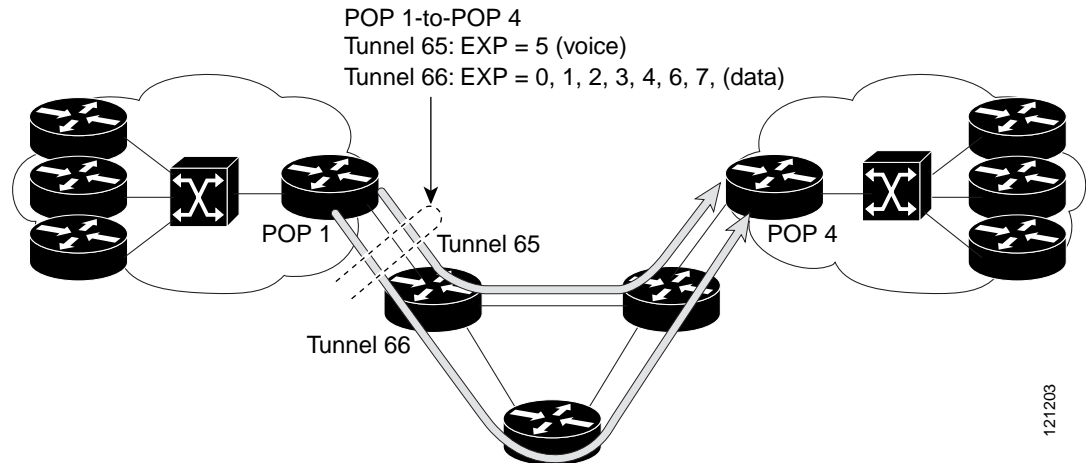
- [Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend, page 10](#)
- [Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel, page 13](#)
- [Making the MPLS TE or DS-TE Tunnels Visible for Routing, page 14](#)
- [Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP, page 15](#)
- [Configuring a Master Tunnel, page 17](#)

You need to configure the CBTS feature only on the tunnel headend. No CBTS configuration is required on the tailend or transit LSR.

## Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend

[Figure 1](#) shows an example of two tunnels, Tunnel 65 and Tunnel 66, transporting different classes of traffic between the same headend and the same tailend.

**Figure 1**      **Tunnels Transporting Different Classes of Service Between the Same Headend and Tailend**



To create multiple MPLS TE or DS-TE tunnels with the same headend and same tailend, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **ip unnumbered *type number***
5. **tunnel destination {*hostname* | *ip-address*}**
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth [sub-pool | global] *bandwidth***
8. **exit**
9. Repeat steps 3 through 8 on the same headend router to create additional tunnels from this headend to the same tailend.
10. **end**

## DETAILED STEPS

|         | Command or Action                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                     |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                            |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                           |
| Step 3  | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 65                                                                                      | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                                                                                                                       |
| Step 4  | <b>ip unnumbered <i>type number</i></b><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 0                                                                            | Enables IP processing on an interface without assigning an explicit IP address to the interface.                                                                                                                                                                                                                                                            |
| Step 5  | <b>tunnel destination {<i>hostname</i>   <i>ip-address</i>}</b><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12                                              | Specifies the destination of the tunnel for this path option.                                                                                                                                                                                                                                                                                               |
| Step 6  | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                                            | Sets the mode of a tunnel to MPLS for TE.                                                                                                                                                                                                                                                                                                                   |
| Step 7  | <b>tunnel mpls traffic-eng bandwidth [<i>sub-pool</i>   <i>global</i>] <i>bandwidth</i></b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 3000 | Configures the bandwidth for the MPLS TE tunnel. If automatic bandwidth is configured for the tunnel, use the <b>tunnel mpls traffic-eng bandwidth</b> command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism.<br><br><b>Note</b> You can configure any existing MPLS TE command on these TE or DS-TE tunnels. |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                            | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                       |
| Step 9  | Repeat steps 3 through 8 on the same headend router to create additional tunnels from this headend to the same tailend.                                                                  | —                                                                                                                                                                                                                                                                                                                                                           |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                 | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                            |

## Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel

To configure EXP values to be carried by each MPLS TE or DS-TE tunnel, perform the following steps. For each tunnel that you create, you must indicate which EXP values the tunnel carries.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel mpls traffic-eng exp** [*list-of-exp-values*] [**default**]
5. **exit**
6. Repeat steps 3 through 5 for all MPLS TE tunnels that you created in the [“Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend”](#) section on page 10.
7. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                              | Purpose                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                 |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 65                                                              | Configures an interface type and enters interface configuration mode.                                             |
| Step 4 | <b>tunnel mpls traffic-eng exp</b> [ <i>list-of-exp-values</i> ] [ <b>default</b> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng exp 5 | Specifies the EXP bits that will be forwarded over a member tunnel that is part of the CBTS bundle.               |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                  | Returns to global configuration mode.                                                                             |

|        | Command or Action                                                                                                                                                                                   | Purpose                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Step 6 | Repeat steps 3 through 5 for all MPLS TE tunnels that you created in the <a href="#">“Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend”</a> section on page 10. | —                                |
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-if)# end</code>                                                                                                                      | Returns to privileged EXEC mode. |

## Making the MPLS TE or DS-TE Tunnels Visible for Routing

Perform the following task to make the MPLS TE or DS-TE tunnels visible for routing.



### Note

Alternatively, static routing could be used instead of `autoroute` to make the TE or DS-TE tunnels visible for routing.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type number`
4. `tunnel mpls traffic-eng autoroute announce`
5. `tunnel mpls traffic-eng autoroute metric {absolute | relative} value`
6. `end`

### DETAILED STEPS

|        | Command or Action                                                                                             | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>             | Enters global configuration mode.                                                                                  |
| Step 3 | <code>interface type number</code><br><br><b>Example:</b><br><code>Router(config)# interface tunnel 65</code> | Configures an interface type and enters interface configuration mode.                                              |

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>tunnel mpls traffic-eng autoroute announce</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng autoroute announce                                    | Specifies that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 5 | <b>tunnel mpls traffic-eng autoroute metric {absolute   relative} value</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng autoroute metric relative 2 | Specifies the MPLS TE tunnel metric that the IGP enhanced SPF calculation uses.<br><br><b>Note</b> 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 the metric to the tunnel tailend appears to be 4 from the routing table, then the cost to the tunnel tailend 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. |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP

To verify that the MPLS TE or DS-TE tunnels are operating and announced to the IGP, perform the following steps.

### SUMMARY STEPS

1. **show mpls traffic-eng topology** {ip-address | igp-id {isis nsap-address | ospf ip-address}} [brief]
2. **show mpls traffic-eng tunnels** number [brief] protect
3. **show ip cef** [vrf vrf-name] [unresolved [detail] | [detail | summary]]
4. **show mpls forwarding-table** [network {mask | length} | labels label [- label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]
5. **show mpls traffic-eng autoroute**

### DETAILED STEPS

- Step 1** **show mpls traffic-eng topology** {ip-address | igp-id {isis nsap-address | ospf ip-address}} [brief]

Use this command to display the MPLS TE global topology currently known at this node:

```
Router# show mpls traffic-eng topology
```

```
My_System_id: 0000.0025.0003.00
```

```

IGP Id: 0000.0024.0004.00, MPLS TE Id:172.16.4.4 Router Node
  link[0 ]:Intf Address: 10.1.1.4
    Nbr IGP Id: 0000.0024.0004.02,
    admin_weight:10, affinity_bits:0x0
    max_link_bw:10000 max_link_reservable: 10000
  globalpoolsubpool
    total allocatedreservable reservable
  -----
bw[0]: 0 1000500
bw[1]:10 990490
bw[2]: 600 390390
bw[3]: 0 390390
bw[4]: 0 390390
bw[5]: 0 390390

```

## Step 2 show mpls traffic-eng tunnels *number* [brief] [protection]

Use this command to display information for a specified tunneling interface:

```
Router# show mpls traffic-eng tunnels 500 brief protection
```

```

Router#_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 172.16.0.5, Dest 172.16.0.8, Instance 17
Fast Reroute Protection: None
Path Protection: 1 Common Link(s) , 1 Common Node(s)
  Primary lsp path:192.168.6.6 192.168.7.7
                  192.168.8.8 192.168.0.8

  Protect lsp path:172.16.7.7 192.168.8.8
                  10.0.0.8
Path Protect Parameters:
  Bandwidth: 50      kbps (Global)  Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
InLabel : -
OutLabel : Serial5/3, 46
RSVP Signalling Info:
  Src 172.16.0.5, Dst 172.16.0.8, Tun_Id 500, Tun_Instance 18
RSVP Path Info:
  My Address: 172.16.0.5
  Explicit Route: 192.168.7.7 192.168.8.8
  Record Route: NONE
  Tspec: ave rate=50 kbits, burst=1000 bytes, peak rate=50 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=50 kbits, burst=1000 bytes, peak rate=50 kbits

```

## Step 3 show ip cef summary

Use this command to display a summary of the IP CEF table:

```
Router# show ip cef summary
```

```

IP Distributed CEF with switching (Table Version 25), flags=0x0
21 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 1
21 leaves, 16 nodes, 19496 bytes, 36 inserts, 15 invalidations
0 load sharing elements, 0 bytes, 0 references
universal per-destination load sharing algorithm, id 5163EC15
3(0) CEF resets, 0 revisions of existing leaves
Resolution Timer: Exponential (currently 1s, peak 1s)
0 in-place/0 aborted modifications
refcounts: 4377 leaf, 4352 node

Table epoch: 0 (21 entries at this epoch)

```



Adjacency Table has 9 adjacencies

**Step 4** **show mpls forwarding-table** [*network {mask | length}*] | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*] [**vrf** *vrf-name*] [**detail**]

Use this command to display the contents of the MPLS Label Forwarding Information Base (LFIB):

Router# **show mpls forwarding-table**

| Local Label | Outgoing Label or VC | Prefix or Tunnel Id | Bytes switched | tag | Outgoing interface | Next Hop    |
|-------------|----------------------|---------------------|----------------|-----|--------------------|-------------|
| 26          | No Label             | 10.253.0.0/16       | 0              |     | Et4/0/0            | 10.27.32.4  |
| 28          | 1/33                 | 10.15.0.0/16        | 0              |     | AT0/0.1            | point2point |
| 29          | Pop Label            | 10.91.0.0/16        | 0              |     | Hs5/0              | point2point |
|             | 1/36                 | 10.91.0.0/16        | 0              |     | AT0/0.1            | point2point |
| 30          | 32                   | 10.250.0.97/32      | 0              |     | Et4/0/2            | 10.92.0.7   |
|             | 32                   | 10.250.0.97/32      | 0              |     | Hs5/0              | point2point |
| 34          | 26                   | 10.77.0.0/24        | 0              |     | Et4/0/2            | 10.92.0.7   |
|             | 26                   | 10.77.0.0/24        | 0              |     | Hs5/0              | point2point |
| 35          | No Label[T]          | 10.100.100.101/32   | 0              |     | Tu301              | point2point |
| 36          | Pop Label            | 10.1.0.0/16         | 0              |     | Hs5/0              | point2point |
|             | 1/37                 | 10.1.0.0/16         | 0              |     | AT0/0.1            | point2point |

[T] Forwarding through a TSP tunnel.  
View additional tagging info with the 'detail' option

**Step 5** **show mpls traffic-eng autoroute**

Use this command to display tunnels that are announced to the IGP, including interface, destination, and bandwidth:

Router# **show mpls traffic-eng autoroute**

```
MPLS TE autorouting enabled
destination 0002.0002.0002.00 has 2 tunnels
  Tunnell021 (traffic share 10000, nexthop 10.2.2.2, absolute metric 11)
  Tunnell022 (traffic share 3333, nexthop 10.2.2.2, relative metric -3)
destination 0003.0003.0003.00 has 2 tunnels
  Tunnell032 (traffic share 10000, nexthop 172.16.3.3)
  Tunnell031 (traffic share 10000, nexthop 172.16.3.3, relative metric -1)
```

## Configuring a Master Tunnel

To configure a master tunnel to which other tunnels can be members, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **tunnel destination** {*hostname* | *ip-address*}
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng exp-bundle master**

8. **tunnel mpls traffic-eng exp-bundle member** *tunnel-number*

9. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                    | Purpose                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                       | Enters global configuration mode.                                                                                   |
| Step 3 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 65                                                                  | Configures an interface type and enters interface configuration mode.                                               |
| Step 4 | <b>ip unnumbered</b> <i>type number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 0                                                        | Enables IP processing on an interface without assigning an explicit IP address to the interface.                    |
| Step 5 | <b>tunnel destination</b> { <i>hostname</i>   <i>ip-address</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.10.10.12                        | Specifies the destination of the tunnel for this path option.                                                       |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                        | Sets the mode of a tunnel to MPLS for TE.                                                                           |
| Step 7 | <b>tunnel mpls traffic-eng exp-bundle master</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng exp-bundle master                              | Configures a master tunnel.                                                                                         |
| Step 8 | <b>tunnel mpls traffic-eng exp-bundle member</b> <i>tunnel-number</i><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng exp-bundle member tunnel1 | Identifies which tunnel is a member of a master tunnel.                                                             |
| Step 9 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                        | Exits to global configuration mode.                                                                                 |

# Configuration Examples for MPLS Traffic Engineering : Class-based Tunnel Selection

This section contains the following configuration examples:

- [Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend: Example, page 19](#)
- [Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel: Example, page 19](#)
- [Making the MPLS TE or DS-TE Tunnels Visible for Routing: Example, page 20](#)
- [Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP: Example, page 20](#)
- [Configuring a Master Tunnel: Example, page 27](#)

## Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend: Example

The following example shows how to create multiple MPLS TE or DS-TE tunnels from the same headend to the same tailend:

```
Router(config)# interface Tunnel 65
Router(config-if)# ip numbered loopback 0
Router(config-if)# tunnel destination 10.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
Router(config-if)# ^Z
Router(config)# interface Tunnel 66
Router(config-if)# ip numbered loopback 0
Router(config-if)# tunnel destination 10.1.1.1
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng bandwidth 50000
Router(config-if)# end
Router#
```

## Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel: Example

The following example shows how to configure EXP values to be carried by each MPLS TE or DS-TE tunnel that you created:

```
Router(config)# interface Tunnel 65
Router(config-if)# tunnel mpls traffic-eng exp 5
Router(config-if)# ^Z
Router(config)#
Router(config)# interface Tunnel 66
Router(config-if)# tunnel mpls traffic-eng exp 0 1 2 3 4 6 7
Router(config-if)# end
Router#
```

## Making the MPLS TE or DS-TE Tunnels Visible for Routing: Example

The following example shows how to make the MPLS TE or DS-TE tunnels visible for routing:

```
Router(config)# interface Tunnel 65
Router(config-if)# tunnel mpls traffic-eng autoroute announce
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative -2
Router(config-if)# ^Z
Router(config)#
Router(config)# interface Tunnel 66
Router(config-if)# tunnel mpls traffic-eng autoroute announce
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative -2
Router(config-if)# end
Router#
```

Packets destined beyond 10.1.1.1 are sent on:

- Tunnel 65 if their EXP value after input MQC is 5.
- Tunnel 66 if their EXP value after input MQC is 0, 1, 2, 3, 4, 6, or 7.

## Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP: Example

The output for each of the following examples helps verify that the MPLS TE or DS-TE tunnels are operating and visible.

The **show mpls traffic-eng topology** command output displays the MPLS TE global topology:

```
Router# show mpls traffic-eng topology 10.0.0.1
```

```
IGP Id: 10.0.0.1, MPLS TE Id:10.0.0.1 Router Node (ospf 10 area 0) id 1
link[0]: Broadcast, DR: 10.0.1.2, nbr_node_id:6, gen:18
frag_id 0, Intf Address:10.1.1.1
TE metric:1, IGP metric:1, attribute_flags:0x0
SRLGs: None
physical_bw: 100000 (kbps), max_reservable_bw_global: 1000 (kbps)
max_reservable_bw_sub: 0 (kbps)
```

|        | Total Allocated<br>BW (kbps) | Global Pool<br>Reservable<br>BW (kbps) | Sub Pool<br>Reservable<br>BW (kbps) |
|--------|------------------------------|----------------------------------------|-------------------------------------|
| bw[0]: | 0                            | 1000                                   | 0                                   |
| bw[1]: | 0                            | 1000                                   | 0                                   |
| bw[2]: | 0                            | 1000                                   | 0                                   |
| bw[3]: | 0                            | 1000                                   | 0                                   |
| bw[4]: | 0                            | 1000                                   | 0                                   |
| bw[5]: | 0                            | 1000                                   | 0                                   |
| bw[6]: | 0                            | 1000                                   | 0                                   |
| bw[7]: | 100                          | 900                                    | 0                                   |

```
link[1]: Broadcast, DR: 10.0.2.2, nbr_node_id:7, gen:19
frag_id 1, Intf Address:10.0.2.1
TE metric:1, IGP metric:1, attribute_flags:0x0
SRLGs: None
physical_bw: 100000 (kbps), max_reservable_bw_global: 1000 (kbps)
max_reservable_bw_sub: 0 (kbps)
```

|  | Total Allocated | Global Pool<br>Reservable | Sub Pool<br>Reservable |
|--|-----------------|---------------------------|------------------------|
|--|-----------------|---------------------------|------------------------|

|        | BW (kbps) | BW (kbps) | BW (kbps) |
|--------|-----------|-----------|-----------|
|        | -----     | -----     | -----     |
| bw[0]: | 0         | 1000      | 0         |
| bw[1]: | 0         | 1000      | 0         |
| bw[2]: | 0         | 1000      | 0         |
| bw[3]: | 0         | 1000      | 0         |
| bw[4]: | 0         | 1000      | 0         |
| bw[5]: | 0         | 1000      | 0         |
| bw[6]: | 0         | 1000      | 0         |
| bw[7]: | 300       | 700       | 0         |

Router#

Router# **show mpls traffic-eng topology 10.0.0.9**

IGP Id: 10.0.0.9, MPLS TE Id:10.0.0.9 Router Node (ospf 10 area 0) id 3  
 link[0]: Point-to-Point, Nbr IGP Id: 10.0.0.5, nbr\_node\_id:5, gen:9  
 frag\_id 1, Intf Address:10.0.5.2, Nbr Intf Address:10.0.5.1  
 TE metric:1, IGP metric:1, attribute\_flags:0x0  
 SRLGs: None  
 physical\_bw: 155000 (kbps), max\_reservable\_bw\_global: 1000 (kbps)  
 max\_reservable\_bw\_sub: 0 (kbps)

|        | Total Allocated<br>BW (kbps) | Global Pool<br>Reservable<br>BW (kbps) | Sub Pool<br>Reservable<br>BW (kbps) |
|--------|------------------------------|----------------------------------------|-------------------------------------|
|        | -----                        | -----                                  | -----                               |
| bw[0]: | 0                            | 1000                                   | 0                                   |
| bw[1]: | 0                            | 1000                                   | 0                                   |
| bw[2]: | 0                            | 1000                                   | 0                                   |
| bw[3]: | 0                            | 1000                                   | 0                                   |
| bw[4]: | 0                            | 1000                                   | 0                                   |
| bw[5]: | 0                            | 1000                                   | 0                                   |
| bw[6]: | 0                            | 1000                                   | 0                                   |
| bw[7]: | 0                            | 1000                                   | 0                                   |

link[1]: Point-to-Point, Nbr IGP Id: 10.0.0.7, nbr\_node\_id:4, gen:9  
 frag\_id 0, Intf Address:10.0.6.2, Nbr Intf Address:10.0.6.1  
 TE metric:1, IGP metric:1, attribute\_flags:0x0  
 SRLGs: None  
 physical\_bw: 155000 (kbps), max\_reservable\_bw\_global: 1000 (kbps)  
 max\_reservable\_bw\_sub: 0 (kbps)

|        | Total Allocated<br>BW (kbps) | Global Pool<br>Reservable<br>BW (kbps) | Sub Pool<br>Reservable<br>BW (kbps) |
|--------|------------------------------|----------------------------------------|-------------------------------------|
|        | -----                        | -----                                  | -----                               |
| bw[0]: | 0                            | 1000                                   | 0                                   |
| bw[1]: | 0                            | 1000                                   | 0                                   |
| bw[2]: | 0                            | 1000                                   | 0                                   |
| bw[3]: | 0                            | 1000                                   | 0                                   |
| bw[4]: | 0                            | 1000                                   | 0                                   |
| bw[5]: | 0                            | 1000                                   | 0                                   |
| bw[6]: | 0                            | 1000                                   | 0                                   |
| bw[7]: | 0                            | 1000                                   | 0                                   |

Router#

The **show mpls traffic-eng tunnels** command output displays information about a tunnel:

Router# **show mpls traffic-eng tunnels tunnel1**

Name: Router\_t1 (Tunnel1) Destination: 10.0.0.9  
 Status:  
 Admin: up Oper: up Path: valid Signalling: connected  
 path option 1, type explicit path1 (Basis for Setup, path weight 3)

```

Config Parameters:
  Bandwidth: 100          kbps (Global)  Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled    LockDown: disabled  Loadshare: 100      bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled

InLabel  : -
OutLabel : FastEthernet6/0, 12304
RSVP Signalling Info:
  Src 10.0.0.1, Dst 10.0.0.9, Tun_Id 1, Tun_Instance 10
  RSVP Path Info:
    My Address: 10.0.1.1
    Explicit Route: 10.0.1.2 10.0.3.2 10.0.5.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=17179869 kbits
Shortest Unconstrained Path Info:
  Path Weight: 3 (TE)
  Explicit Route: 10.0.2.1 180.0.2.2 10.0.3.2 180.0.5.2
                  10.0.0.9
History:
  Tunnel:
    Time since created: 15 minutes, 18 seconds
    Time since path change: 15 minutes, 5 seconds
  Current LSP:
    Uptime: 15 minutes, 5 seconds

```

Router# **show mpls traffic-eng tunnel tunnel2**

```

Name: Router_t2                                     (Tunnel2) Destination: 10.0.0.9
Status:
  Admin: up      Oper: up      Path: valid      Signalling: connected
  path option 1, type explicit path2 (Basis for Setup, path weight 3)

Config Parameters:
  Bandwidth: 100          kbps (Global)  Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled    LockDown: disabled  Loadshare: 100      bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 1 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled

InLabel  : -
OutLabel : FastEthernet6/1, 12305
RSVP Signalling Info:
  Src 10.0.0.1, Dst 10.0.0.9, Tun_Id 2, Tun_Instance 10
  RSVP Path Info:
    My Address: 10.0.2.1
    Explicit Route: 10.0.2.2 10.0.4.2 10.0.6.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=17179869 kbits
Shortest Unconstrained Path Info:

```

```

Path Weight: 3 (TE)
Explicit Route: 10.0.2.1 10.0.2.2 10.0.3.2 10.0.5.2
                10.0.0.9
History:
Tunnel:
    Time since created: 15 minutes, 19 seconds
    Time since path change: 15 minutes, 6 seconds
Current LSP:
    Uptime: 15 minutes, 6 seconds

```

Router# **show mpls traffic-eng tunnels tunnel3**

```

Name: Router_t3                               (Tunnel3) Destination: 10.0.0.9
Status:
    Admin: up          Oper: up          Path: valid          Signalling: connected
    path option 1, type explicit path2 (Basis for Setup, path weight 3)

Config Parameters:
    Bandwidth: 100      kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: enabled LockDown: disabled Loadshare: 100      bw-based
    auto-bw: disabled
Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : FastEthernet6/1, 12306
RSVP Signalling Info:
    Src 10.0.0.1, Dst 10.0.0.9, Tun_Id 3, Tun_Instance 8
RSVP Path Info:
    My Address: 10.0.2.1
    Explicit Route: 10.0.2.2 10.0.4.2 10.0.6.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=17179869 kbits
Shortest Unconstrained Path Info:
    Path Weight: 3 (TE)
    Explicit Route: 10.0.2.1 10.0.2.2 10.0.3.2 10.0.5.2
                  10.0.0.9
History:
Tunnel:
    Time since created: 15 minutes, 19 seconds
    Time since path change: 15 minutes, 7 seconds
Current LSP:
    Uptime: 15 minutes, 7 seconds

```

Router# **show mpls traffic-eng tunnels tunnel4**

```

Name: Router_t4                               (Tunnel4) Destination: 10.0.0.9
Status:
    Admin: up          Oper: up          Path: valid          Signalling: connected
    path option 1, type explicit path2 (Basis for Setup, path weight 3)

Config Parameters:
    Bandwidth: 100      kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: enabled LockDown: disabled Loadshare: 100      bw-based
    auto-bw: disabled
Active Path Option Parameters:

```

```

State: explicit path option 1 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : FastEthernet6/1, 12307
RSVP Signalling Info:
  Src 10.0.0.1, Dst 10.0.0.9, Tun_Id 4, Tun_Instance 6
  RSVP Path Info:
    My Address: 10.0.2.1
    Explicit Route: 10.0.2.2 10.0.4.2 10.0.6.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=17179869 kbits
Shortest Unconstrained Path Info:
  Path Weight: 3 (TE)
  Explicit Route: 10.0.2.1 10.0.2.2 10.0.3.2 10.0.5.2
                  10.0.0.9
History:
  Tunnel:
    Time since created: 15 minutes, 20 seconds
    Time since path change: 15 minutes, 8 seconds
  Current LSP:
    Uptime: 15 minutes, 8 seconds

```

The **show ip cef detail** command output displays detailed FIB entry information for a tunnel:

```
Router# show ip cef tunnel1 detail
```

```

IP CEF with switching (Table Version 46), flags=0x0
 31 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
 2 instant recursive resolutions, 0 used background process
 8 load sharing elements, 8 references
 6 in-place/0 aborted modifications
34696 bytes allocated to the FIB table data structures
universal per-destination load sharing algorithm, id 9EDD49E1
1(0) CEF resets
Resolution Timer: Exponential (currently 1s, peak 1s)
Tree summary:
 8-8-8-8 stride pattern
short mask protection disabled
31 leaves, 23 nodes using 26428 bytes

Table epoch: 0 (31 entries at this epoch)

Adjacency Table has 13 adjacencies
10.0.0.9/32, version 45, epoch 0, per-destination sharing
0 packets, 0 bytes
  tag information set, all rewrites inherited
    local tag: tunnel head
  via 0.0.0.0, Tunnel1, 0 dependencies
    traffic share 1
    next hop 0.0.0.0, Tunnel1
    valid adjacency
    tag rewrite with Tu1, point2point, tags imposed {12304}
  0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
         internal 0 packets, 0 bytes

```

```
Router# show ip cef tunnel2 detail
```



```

IP CEF with switching (Table Version 46), flags=0x0
 31 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
 2 instant recursive resolutions, 0 used background process
 8 load sharing elements, 8 references
 6 in-place/0 aborted modifications
34696 bytes allocated to the FIB table data structures
universal per-destination load sharing algorithm, id 9EDD49E1
1(0) CEF resets
Resolution Timer: Exponential (currently 1s, peak 1s)
Tree summary:
 8-8-8-8 stride pattern
 short mask protection disabled
31 leaves, 23 nodes using 26428 bytes

```

Table epoch: 0 (31 entries at this epoch)

```

Adjacency Table has 13 adjacencies
10.0.0.9/32, version 45, epoch 0, per-destination sharing
0 packets, 0 bytes
 tag information set, all rewrites inherited
   local tag: tunnel head
via 0.0.0.0, Tunnel2, 0 dependencies
 traffic share 1
 next hop 0.0.0.0, Tunnel2
 valid adjacency
 tag rewrite with Tu2, point2point, tags imposed {12305}
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
         internal 0 packets, 0 bytes

```

Router# **show ip cef tunnel3 detail**

```

IP CEF with switching (Table Version 46), flags=0x0
 31 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
 2 instant recursive resolutions, 0 used background process
 8 load sharing elements, 8 references
 6 in-place/0 aborted modifications
34696 bytes allocated to the FIB table data structures
universal per-destination load sharing algorithm, id 9EDD49E1
1(0) CEF resets
Resolution Timer: Exponential (currently 1s, peak 1s)
Tree summary:
 8-8-8-8 stride pattern
 short mask protection disabled
31 leaves, 23 nodes using 26428 bytes

```

Table epoch: 0 (31 entries at this epoch)

```

Adjacency Table has 13 adjacencies
10.0.0.9/32, version 45, epoch 0, per-destination sharing
0 packets, 0 bytes
 tag information set, all rewrites inherited
   local tag: tunnel head
via 0.0.0.0, Tunnel3, 0 dependencies
 traffic share 1
 next hop 0.0.0.0, Tunnel3
 valid adjacency
 tag rewrite with Tu3, point2point, tags imposed {12306}
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
         internal 0 packets, 0 bytes

```

```
Router# show ip cef tunnel4 detail
```

```
IP CEF with switching (Table Version 46), flags=0x0
 31 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 2
 2 instant recursive resolutions, 0 used background process
 8 load sharing elements, 8 references
 6 in-place/0 aborted modifications
 34696 bytes allocated to the FIB table data structures
 universal per-destination load sharing algorithm, id 9EDD49E1
 1(0) CEF resets
 Resolution Timer: Exponential (currently 1s, peak 1s)
 Tree summary:
   8-8-8-8 stride pattern
   short mask protection disabled
   31 leaves, 23 nodes using 26428 bytes

Table epoch: 0 (31 entries at this epoch)

Adjacency Table has 13 adjacencies
10.0.0.9/32, version 45, epoch 0, per-destination sharing
0 packets, 0 bytes
 tag information set, all rewrites inherited
   local tag: tunnel head
 via 0.0.0.0, Tunnel4, 0 dependencies
   traffic share 1
   next hop 0.0.0.0, Tunnel4
   valid adjacency
   tag rewrite with Tu4, point2point, tags imposed {12307}
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
         internal 0 packets, 0 bytes
```

The **show mpls forwarding-table detail** command output displays detailed information from the MPLS LFIB:

```
Router# show mpls forwarding-table detail
```

| Local tag                                                                                                                                                  | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------|--------------------|--------------------|-------------|
| Tun hd                                                                                                                                                     | Untagged           | 10.0.0.9/32         | 0                  | Tu1                | point2point |
| MAC/Encaps=14/18, MRU=1500, Tag Stack{12304}, via Fa6/0<br>00027D88400000ED70178A88847 03010000<br>No output feature configured<br>Per-exp selection: 1    |                    |                     |                    |                    |             |
|                                                                                                                                                            | Untagged           | 10.0.0.9/32         | 0                  | Tu2                | point2point |
| MAC/Encaps=14/18, MRU=1500, Tag Stack{12305}, via Fa6/1<br>00027D884001000ED70178A98847 03011000<br>No output feature configured<br>Per-exp selection: 2 3 |                    |                     |                    |                    |             |
|                                                                                                                                                            | Untagged           | 10.0.0.9/32         | 0                  | Tu3                | point2point |
| MAC/Encaps=14/18, MRU=1500, Tag Stack{12306}, via Fa6/1<br>00027D884001000ED70178A98847 03012000<br>No output feature configured<br>Per-exp selection: 4 5 |                    |                     |                    |                    |             |
|                                                                                                                                                            | Untagged           | 10.0.0.9/32         | 0                  | Tu4                | point2point |
| MAC/Encaps=14/18, MRU=1500, Tag Stack{12307}, via Fa6/1<br>00027D884001000ED70178A98847 03013000                                                           |                    |                     |                    |                    |             |

```
No output feature configured
Per-exp selection: 0 6 7
Router#
```

The **show mpls traffic-eng autoroute** command output displays tunnels that are announced to the IGP:

```
Router# show mpls traffic-eng autoroute

MPLS TE autorouting enabled
destination 10.0.0.9, area ospf 10 area 0, has 4 tunnels
  Tunnel1      (load balancing metric 20000000, nexthop 10.0.0.9)
                (flags: Announce)
  Tunnel2      (load balancing metric 20000000, nexthop 10.0.0.9)
                (flags: Announce)
  Tunnel3      (load balancing metric 20000000, nexthop 10.0.0.9)
                (flags: Announce)
  Tunnel4      (load balancing metric 20000000, nexthop 10.0.0.9)
                (flags: Announce)
Router#
```

## Configuring a Master Tunnel: Example

The following example specifies that there is a master tunnel that includes tunnels Tunnel20000 through Tunnel20005:

```
interface Tunnel 200
 ip unnumbered Loopback 0
 tunnel destination 10.10.10.10
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel20000
 tunnel mpls traffic-eng exp-bundle member Tunnel20001
 tunnel mpls traffic-eng exp-bundle member Tunnel20002
 tunnel mpls traffic-eng exp-bundle member Tunnel20003
 tunnel mpls traffic-eng exp-bundle member Tunnel20004
 tunnel mpls traffic-eng exp-bundle member Tunnel20005
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering (TE): Class-based Tunnel Selection feature.

### Related Documents

| Related Topic                     | Document Title                                                            |
|-----------------------------------|---------------------------------------------------------------------------|
| MPLS traffic engineering commands | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **show ip cef**
- **show mpls forwarding-table**
- **show mpls traffic-eng tunnels**
- **tunnel mpls traffic-eng exp**
- **tunnel mpls traffic-eng exp-bundle master**
- **tunnel mpls traffic-eng exp-bundle member**

# Feature Information for MPLS Traffic Engineering : Class-based Tunnel Selection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering : Class-based Tunnel Selection

| Feature Name                                            | Releases                                                           | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering : Class-based Tunnel Selection | 12.0(29)S<br>12.2(33)SRA<br>12.2(32)SY<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS Traffic Engineering (TE): Class-based Tunnel Selection feature enables you to dynamically route and forward traffic with different class of service (CoS) values onto different TE tunnels between the same tunnel headend and the same tailend. The TE tunnels can be regular TE or DiffServ-aware TE (DS-TE) tunnels.</p> <p>In 12.0(29)S, this feature was introduced.</p> <p>In 12.2(33)SRA, this feature was integrated and the following commands were added:</p> <ul style="list-style-type: none"> <li><b>tunnel mpls traffic-eng exp-bundle master</b></li> <li><b>tunnel mpls traffic-eng exp-bundle member</b></li> </ul> <p>12.0(32)SY, support for this feature was added on the Cisco 12000 family of routers.</p> <p>In 12.2(33)SXH, this feature was integrated.</p> <p>In 12.4(20)T, this feature was integrated.</p> |

# Glossary

**BGP**—Border Gateway Protocol. Interdomain routing protocol that replaces External Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 116.3

**bundled tunnels**—Members of a master tunnel. You define the EXP bits that will be forwarded over each bundled tunnel.

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with large and dynamic traffic patterns, such as the Internet and networks characterized by intensive web-based applications or interactive sessions.

**CoS**—class of service. An indication of how an upper-layer protocol requires a lower-layer protocol to treat its messages. In Systems Network Architecture (SNA) subarea routing, CoS definitions are used by subarea nodes to determine the optimal route for establishing a given session. A CoS definition comprises a virtual route number and a transmission priority field. Also called type of service (ToS).

**DS-TE**—DiffServ-aware traffic engineering. The configuring of two bandwidth pools on each link, a global pool and a subpool. Multiprotocol Label Switching (MPLS) traffic engineering tunnels using the subpool bandwidth can be configured with quality of service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network. Simultaneously, tunnels using the global pool can convey DiffServ traffic.

**EXP**—experimental field or bits. A 3-bit field in the Multiprotocol Label Switching (MPLS) header widely known as the EXP field or EXP bits because, according to RFC 3032, that field is reserved for experimental use. However, the most common use of those bits is for quality of service (QoS) purposes.

**headend**—The upstream, transmitting end of a tunnel. This is the first router in the label switched path (LSP).

**LSP**—label switched path. A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through label switching mechanisms. A label switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**master tunnel**—A set of tunnels that have the same destination.

**MPLS traffic engineering**—Multiprotocol Label Switching traffic engineering. A constraint-based routing algorithm for routing label switched path (LSP) tunnels.

**MQC**—modular quality of service (QoS) command-line interface (CLI). A CLI structure that allows users to create traffic polices and attach those polices to interfaces.

**PBR**—policy-based routing. A routing scheme in which packets are forwarded to specific interfaces based on user-configured policies. A policy might specify, for example, that traffic sent from a particular network should be forwarded out one interface, and all other traffic should be forwarded out another interface.

**tailend**—The downstream, receiving end of a tunnel. The router that terminates the traffic engineering label switched path (LSP).

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**ToS**—type of service. See CoS.

**tunnel**—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

**VCD**—virtual circuit descriptor. A unique number for each ATM interface processor (AIP) that tells the AIP which virtual path identifier (VPI)/virtual channel identifier (VCI) to use for a particular packet. Valid values range from 1 to the value set with the **atm maxvc** command.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

© 2003–2008 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering: Interarea Tunnels

---

**First Published: January 16, 2003**

**Last Updated: October 21, 2009**

The MPLS Traffic Engineering: Interarea Tunnels feature allows you to establish Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels that span multiple Interior Gateway Protocol (IGP) areas and levels, removing the restriction that had required the tunnel headend and tailend routers both be in the same area. The IGP can be either Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).



**Note**

---

Cisco IOS Release 12.2(33)SRE and later releases support the autoroute destination feature, which automatically routes traffic through TE tunnels instead of through manually configured static routes.

---

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering: Interarea Tunnels”](#) section on [page 25](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering: Interarea Tunnels, page 2](#)
- [Restrictions for MPLS Traffic Engineering: Interarea Tunnels, page 2](#)
- [Information About MPLS Traffic Engineering: Interarea Tunnels, page 2](#)
- [How to Configure MPLS Traffic Engineering: Interarea Tunnels, page 5](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for MPLS Traffic Engineering: Interarea Tunnels, page 18](#)
- [Additional References, page 23](#)
- [Feature Information for MPLS Traffic Engineering: Interarea Tunnels, page 25](#)
- [Glossary, page 26](#)

## Prerequisites for MPLS Traffic Engineering: Interarea Tunnels

Your network must support the following Cisco IOS features:

- MPLS
- IP Cisco Express Forwarding
- IS-IS or OSPF
- TE tunnels

## Restrictions for MPLS Traffic Engineering: Interarea Tunnels

- The dynamic path option feature for TE tunnels (which is specified in the **tunnel mpls traffic-eng path-option *number* dynamic** command) is not supported for interarea tunnels. An explicit path identifying the Area Border Routers (ABRs) is required. When there are choices for the ABRs to be used, multiple explicit paths are recommended, each of which identifies a different sequence of ABRs.
- The MPLS TE AutoRoute feature (which is specified in the **tunnel mpls traffic-eng autoroute announce** command) is not supported for interarea tunnels because you would need to know the network topology behind the tailend router.
- Tunnel affinity (the **tunnel mpls traffic-eng affinity** command) is not supported for interarea tunnels.
- The reoptimization of tunnel paths is not supported for interarea tunnels.
- Cisco IOS Release 12.4(20)T does not support stateful switchover (SSO) recovery of label-switched paths (LSPs) that include loose hops.

## Information About MPLS Traffic Engineering: Interarea Tunnels

Before using the MPLS Traffic Engineering: Interarea Tunnels feature, you need to understand the following concepts:

- [Interarea Tunnels Functionality, page 3](#)
- [Autoroute Destination Functionality, page 4](#)
- [MPLS Traffic Engineering Interarea Tunnels Benefits, page 5](#)

## Interarea Tunnels Functionality

To configure an interarea tunnel, you specify on the headend router a loosely routed explicit path for the tunnel label switched path (LSP) that identifies each ABR the LSP should traverse using the **next-address loose** command. The headend router and the ABRs along the specified explicit path expand the loose hops, each computing the path segment to the next ABR or tunnel destination.

For example, to configure a TE tunnel from router R1 to router R3 in the simple multiarea network shown in [Figure 1](#), you would specify ABR1 and ABR2 as loose hops in the explicit path for the tunnel.

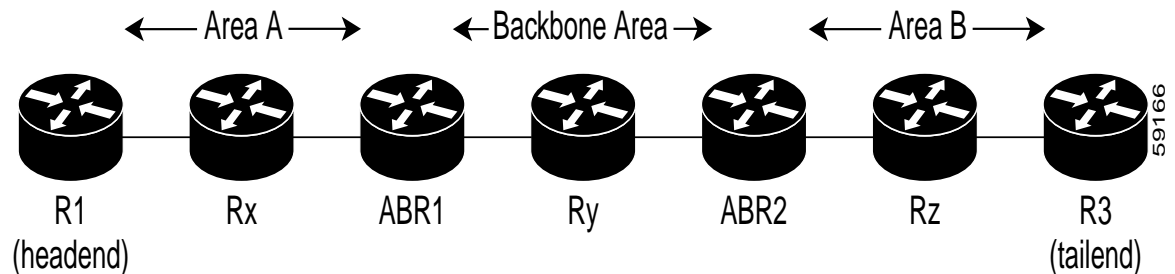


### Note

Rx can be configured as a loose hop as well. In that case, the headend router R1 computes the path to Rx and router Rx computes the path to ABR1.

To signal the tunnel LSP, the headend router (R1) computes the path to ABR1 and sends a Resource Reservation Protocol (RSVP) Path message specifying the path from itself to ABR1 as a sequence of strict hops followed by the path from ABR1 to the tailend as a sequence of loose hops (ABR2, R3). When ABR1 receives the Path message, it expands the path across the backbone area to ABR2 and forwards the Path message specifying the path from itself to ABR2 as a sequence of strict hops followed by the path from ABR2 to the tunnel tailend (R3) as a loose hop. When ABR2 receives the Path message, it expands the path across the tailend area to R3 and propagates the Path message specifying the path from itself to R3 as a sequence of strict hops.

**Figure 1** Multiarea Network



### Note

Cisco IOS Release 12.2(33)SRB supports SSO recovery of LSPs that include loose hops.

Cisco IOS Release 12.4(20)T does not support SSO recovery of LSPs that include loose hops.



### Note

Strictly speaking, IS-IS does not have the notion of an ABR. For the purpose of discussing the MPLS Traffic Engineering: Interarea Tunnels feature, an IS-IS level-1-2 router is considered to be an ABR.



### Note

The explicit path for a TE interarea tunnel may contain any number of non-ABR LSPs. Within an area, a combination of loose and strict next IP addresses is allowed. To specify the next IP address in the explicit path, use the **next-address** command.

**Note**

With OSPF, if an area is connected to the backbone through a virtual link, there may be more than two ABRs in the path.

The following MPLS TE features are supported on interarea traffic engineering LSPs:

- Automatic bandwidth adjustment
- Diff-Serve-aware traffic engineering
- Fast reroute link protection
- Policy-based routing
- Static routing

## Autoroute Destination Functionality

The autoroute destination feature allows you to automatically route traffic through a TE tunnel instead of manually configuring static routes.

You enable this feature on a per-tunnel basis by using the **tunnel mpls traffic-eng autoroute destination** command.

The following sections describe how the autoroute destination feature interacts with other features:

- [CBTS Interaction with Autoroute Destination, page 4](#)
- [Manually Configured Static Routes Interaction with Autoroute Destination, page 4](#)
- [Autoroute Announce Interaction with Autoroute Destination, page 5](#)
- [Forwarding Adjacency Interaction with Autoroute Destination, page 5](#)

## CBTS Interaction with Autoroute Destination

TE tunnels that have the autoroute destination feature enabled can also be configured as class-based traffic shaping (CBTS) tunnel bundle masters or members. Within a CBTS bundle, only the master tunnel with autoroute destination enabled is installed into the Routing Information Base (RIB); that is, the member tunnels are not installed into the RIB.

If member tunnels that have autoroute destination enabled are unconfigured from the bundle, they become regular TE tunnels and TE requests that the static process installs static routes over those tunnels in the RIB. Conversely, when regular TE tunnels with autoroute destination enabled are added to a CBTS bundle as members, TE requests that the static process removes the automatic static routes over those tunnels from the RIB.

## Manually Configured Static Routes Interaction with Autoroute Destination

If there is a manually configured static route to the same destination as a tunnel with autoroute destination enabled via the **tunnel mpls traffic-eng autoroute destination** command, traffic for that destination is load-shared between the static route and the tunnel with autoroute destination enabled.

## Autoroute Announce Interaction with Autoroute Destination

For intra-area tunnels, if a tunnel is configured with both autoroute announce and autoroute destination, the tunnel is announced to the RIB by both the IGP and the static process. RIBs prefer static routes, not IGP routes, so the autoroute destination features takes precedence over autoroute announce.

## Forwarding Adjacency Interaction with Autoroute Destination

If a tunnel is configured with both forwarding adjacency and autoroute destination, the tunnel is announced to the RIB by both the IGP and the static process. The RIB prefers the static route. However, because the IGP was notified about the tunnel via the **forwarding adjacency** command and the tunnel information was flooded, forwarding adjacency continues to function.

## MPLS Traffic Engineering Interarea Tunnels Benefits

- When it is desirable for the traffic from one router to another router in a different IGP area to travel over TE LSPs, the MPLS Traffic Engineering: Interarea Tunnels feature allows you to configure a tunnel that runs from the source router to the destination router. The alternative would be to configure a sequence of tunnels, each crossing one of the areas between source and destination routers such that the traffic arriving on one such tunnel is forwarded into the next such tunnel.
- The autoroute destination feature prevents you from having to manually configure static routes to route traffic over certain interarea tunnels such as ASBRs.

## How to Configure MPLS Traffic Engineering: Interarea Tunnels

This section contains the following tasks:

- [Configuring OSPF for Interarea Tunnels, page 5](#) (optional)
- [Configuring IS-IS for Interarea Tunnels, page 8](#) (optional)
- [Configuring MPLS and RSVP to Support Traffic Engineering, page 12](#) (required)
- [Configuring an MPLS Traffic Engineering Interarea Tunnel, page 14](#) (required)

**Note**

You must configure either OSPF or IS-IS.

## Configuring OSPF for Interarea Tunnels

This section describes the following tasks:

- [Configuring OSPF for ABR Routers, page 6](#)
- [Configuring OSPF for Non-ABR Routers, page 7](#)

## Configuring OSPF for ABR Routers

For each ABR that is running OSPF, perform the following steps to configure traffic engineering on each area you want tunnels in or across. By having multiple areas and configuring traffic engineering in and across each area, the router can contain changes within the network within an area.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **network** *ip-address wildcard-mask* **area** *area-id*
5. **mpls traffic-eng router-id** *interface-name*
6. **mpls traffic-eng area** **0**
7. **mpls traffic-eng area** *number*
8. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router ospf</b> <i>process-id</i><br><br><b>Example:</b><br>Router(config)# router ospf 1                                                                          | Enables OSPF and enters router configuration mode.<br><br>The <i>process-id</i> argument is an internally used identification parameter for the OSPF routing process. It is logically assigned and can be any positive integer. Assign a unique value for each OSPF routing process.                         |
| Step 4 | <b>network</b> <i>ip-address wildcard-mask</i> <b>area</b> <i>area-id</i><br><br><b>Example:</b><br>Router(config-router)# network 192.168.45.0<br>0.0.255.255 area 1 | Specifies the interfaces on which OSPF is to run and specifies the area to which the interface is connected.                                                                                                                                                                                                 |
| Step 5 | <b>mpls traffic-eng router-id</b> <i>interface-name</i><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng<br>router-id Loopback0                      | Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.<br><br>The router identifier is displayed in the <b>show mpls traffic-eng topology path</b> command output.<br><br><b>Note</b> The <i>interface-name</i> value must be Loopback0. |

|        | Command or Action                                                              | Purpose                                                                                                                                 |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <code>mpls traffic-eng area 0</code>                                           | Turns on MPLS traffic engineering for OSPF in area 0.                                                                                   |
|        | <b>Example:</b><br>Router(config-router)# <code>mpls traffic-eng area 0</code> | <b>Note</b> To display the MPLS TE global topology currently known at this node, use the <b>show mpls traffic-eng topology</b> command. |
| Step 7 | <code>mpls traffic-eng area number</code>                                      | Configures a router running OSPF MPLS to flood traffic engineering for the indicated OSPF area.                                         |
|        | <b>Example:</b><br>Router(config-router)# <code>mpls traffic-eng area 2</code> |                                                                                                                                         |
| Step 8 | <code>end</code>                                                               | Returns to privileged EXEC mode.                                                                                                        |
|        | <b>Example:</b><br>Router(config-router)# <code>end</code>                     |                                                                                                                                         |

## Configuring OSPF for Non-ABR Routers

For each non-ABR that is running OSPF, perform the following steps to configure OSPF.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router ospf process-id`
4. `network ip-address wildcard-mask area area-id`
5. `mpls traffic-eng router-id interface-name`
6. `mpls traffic-eng area number`
7. `end`

### DETAILED STEPS

|        | Command or Action                                             | Purpose                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                           | Enables privileged EXEC mode.                                                                                                                                                                                            |
|        | <b>Example:</b><br>Router> <code>enable</code>                | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                     |
| Step 2 | <code>configure terminal</code>                               | Enters global configuration mode.                                                                                                                                                                                        |
|        | <b>Example:</b><br>Router# <code>configure terminal</code>    |                                                                                                                                                                                                                          |
| Step 3 | <code>router ospf process-id</code>                           | Enables OSPF and enters router configuration mode.                                                                                                                                                                       |
|        | <b>Example:</b><br>Router(config)# <code>router ospf 1</code> | The <i>process-id</i> argument is an internally used identification parameter for the OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process. |

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>network</b> <i>ip-address wildcard-mask area area-id</i><br><br><b>Example:</b><br>Router(config-router)# network 192.168.10.10<br>255.255.255.0 area 1 | Specifies the interfaces on which OSPF is to run and specifies the area to which the interface is connected.                                                                                                                                                                                                 |
| Step 5 | <b>mpls traffic-eng router-id interface-name</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng<br>router-id Loopback0                  | Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.<br><br>The router identifier is displayed in the <b>show mpls traffic-eng topology path</b> command output.<br><br><b>Note</b> The <i>interface-name</i> value must be Loopback0. |
| Step 6 | <b>mpls traffic-eng area number</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng area 1                                               | Specifies the area that the router is in.<br><br><b>Note</b> To display the MPLS TE global topology currently known at this node, use the <b>show mpls traffic-eng topology</b> command.                                                                                                                     |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                            | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                             |

## Configuring IS-IS for Interarea Tunnels

This section describes the following tasks:

- [Configuring IS-IS for Backbone Routers, page 8](#)
- [Configuring IS-IS for Nonbackbone Routers, page 10](#)
- [Configuring IS-IS for Interfaces, page 11](#)

## Configuring IS-IS for Backbone Routers

To configure IS-IS for background (level-1-2) routers, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **net nn.nnnn.nnnn.nnnn.nnnn**
6. **mpls traffic-eng router-id interface-name**
7. **mpls traffic-eng level-1**
8. **mpls traffic-eng level-2**
9. **interface typeslot/port**
10. **ip router isis**



11. end

## DETAILED STEPS

|        | Command or Action                                                                                                                         | Purpose                                                                                                                                                                                                |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                                                                                                      |
| Step 3 | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis                                                                  | Enables IS-IS routing and specifies an IS-IS process for IP, and places the router in router configuration mode.                                                                                       |
| Step 4 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                                               | Configures a router to generate and accept only new-style type, length, value objects (TLVs).                                                                                                          |
| Step 5 | <b>net nn.nnnn.nnnn.nnnn.nnnn</b><br><br><b>Example:</b><br>Router(config-router)# net<br>10.0000.0100.0000.0010                          | Configures the area ID (area address) and the system ID.                                                                                                                                               |
| Step 6 | <b>mpls traffic-eng router-id interface-name</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng<br>router-id Loopback0 | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0.                                                                           |
| Step 7 | <b>mpls traffic-eng level-1</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng level-1                                 | Turns on MPLS traffic engineering for IS-IS at level 1.<br><br><b>Note</b> To display the MPLS TE global topology currently known at this node, use the <b>show mpls traffic-eng topology</b> command. |
| Step 8 | <b>mpls traffic-eng level-2</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng level-2                                 | Turns on MPLS traffic engineering for IS-IS at level 2.<br><br><b>Note</b> To display the MPLS TE global topology currently known at this node, use the <b>show mpls traffic-eng topology</b> command. |
| Step 9 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config-router)# interface POS1/0                                          | Configures an interface type and enters interface configuration mode.                                                                                                                                  |

|         | Command or Action                                                                 | Purpose                                                                                              |
|---------|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| Step 10 | <b>ip router isis</b><br><br><b>Example:</b><br>Router(config-if)# ip router isis | Enables IS-IS routing.<br><br>Specify this command on each interface on which you want to run IS-IS. |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                       | Returns to privileged EXEC mode.                                                                     |

## Configuring IS-IS for Nonbackbone Routers

To configure IS-IS for nonbackbone routers, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **net nn.nnnn.nnnn.nnnn.nnnn**
6. **mpls traffic-eng router-id interface-name**
7. **mpls traffic-eng {level-1 | level-2}**
8. **end**

### DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                            |
|--------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                  |
| Step 3 | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis                    | Enables IS-IS routing and specifies an IS-IS process for IP, and places the router in router configuration mode.   |
| Step 4 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide | Configures a router to generate and accept only new-style TLVs.                                                    |

|        | Command or Action                                                                                                                                | Purpose                                                                                                                                                                                                |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>net</b> <i>nn.nnnn.nnnn.nnnn.nnnn</i><br><br><b>Example:</b><br>Router(config-router)# net<br>10.0000.2000.0100.0001                          | Configures the area ID (area address) and the system ID.                                                                                                                                               |
| Step 6 | <b>mpls traffic-eng router-id</b> <i>interface-name</i><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng<br>router-id Loopback0 | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0.                                                                           |
| Step 7 | <b>mpls traffic-eng</b> { <b>level-1</b>   <b>level-2</b> }<br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng level-1            | Turns on MPLS traffic engineering for IS-IS at level 1.<br><br><b>Note</b> To display the MPLS TE global topology currently known at this node, use the <b>show mpls traffic-eng topology</b> command. |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                  | Returns to privileged EXEC mode.                                                                                                                                                                       |

## Configuring IS-IS for Interfaces

To configure IS-IS for interfaces, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **net** *nn.nnnn.nnnn.nnnn.nnnn*
6. **mpls traffic-eng router-id** *interface-name*
7. **interface** *typeslot/port*
8. **ip router isis**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                         | Purpose                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                            |
| Step 3 | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis                                                                  | Enables IS-IS routing and specifies an IS-IS process for IP. This command places the router in router configuration mode.    |
| Step 4 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                                               | Configures a router to generate and accept only new-style TLVs.                                                              |
| Step 5 | <b>net nn.nnnn.nnnn.nnnn.nnnn</b><br><br><b>Example:</b><br>Router(config-router)# net<br>10.0000.0100.0000.0010                          | Configures the area ID (area address) and the system ID.                                                                     |
| Step 6 | <b>mpls traffic-eng router-id interface-name</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng<br>router-id Loopback0 | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0. |
| Step 7 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config-router)# interface POS1/0                                          | Specifies the interface and enters interface configuration mode.                                                             |
| Step 8 | <b>ip router isis</b><br><br><b>Example:</b><br>Router(config-if)# ip router isis                                                         | Enables IS-IS routing.<br><br>Specify this command on each interface on which you want to run IS-IS.                         |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                               | Returns to privileged EXEC mode.                                                                                             |

## Configuring MPLS and RSVP to Support Traffic Engineering

To configure MPLS and RSVP to support traffic engineering on the routers, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **mpls traffic-eng tunnels**
5. **interface** *typeslot/port*
6. **ip address** *ip-address mask* [**secondary** [**vrf** *vrf-name*]]
7. **ip rsvp bandwidth**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                       | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip cef</b><br><br><b>Example:</b><br>Router(config)# ip cef                                                                                                                       | Enables Cisco Express Forwarding on the Route Processor card.                                                    |
| Step 4 | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng tunnels                                                                                   | Enables MPLS traffic engineering tunnel signaling on a device.                                                   |
| Step 5 | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface Loopback0                                                                                  | Specifies the interface and enters interface configuration mode.                                                 |
| Step 6 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> [ <b>vrf</b> <i>vrf-name</i> ]]<br><br><b>Example:</b><br>Router(config-if)# ip address<br>192.168.10.10 255.255.255.255 | Assigns an IP network address and network mask to the interface.                                                 |

|        | Command or Action                                                                             | Purpose                              |
|--------|-----------------------------------------------------------------------------------------------|--------------------------------------|
| Step 7 | <code>ip rsvp bandwidth</code><br><br><b>Example:</b><br>Router(config-if)# ip rsvp bandwidth | Enables RSVP for IP on an interface. |
| Step 8 | <code>end</code><br><br><b>Example:</b><br>Router(config-if)# end                             | Returns to privileged EXEC mode.     |

## Configuring an MPLS Traffic Engineering Interarea Tunnel

This section includes the following tasks:

- [Configuring an MPLS Traffic Engineering Interarea Tunnel to Use Explicit Paths, page 14](#)
- [Configuring Explicit Paths, page 16](#)

### Configuring an MPLS Traffic Engineering Interarea Tunnel to Use Explicit Paths

To configure an MPLS traffic engineering interarea tunnel to use explicit paths, perform the following steps.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel-interface`
4. `ip unnumbered type number`
5. `tunnel destination ip-address`
6. `tunnel mode mpls traffic-eng`
7. `tunnel mpls traffic-eng bandwidth bandwidth`
8. `tunnel mpls traffic-eng path-option number explicit { name path-name | identifier path-number } [lockdown]`
9. `end`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                 |
| Step 3 | <b>interface</b> <i>tunnel-interface</i><br><br><b>Example:</b><br>Router(config)# interface Tunell                                                                                                                                                                  | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                                             |
| Step 4 | <b>ip unnumbered</b> <i>type number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered Loopback 0                                                                                                                                                        | Gives the tunnel interface an IP address.<br><br>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.                                                                                                                   |
| Step 5 | <b>tunnel destination</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 192.168.20.20                                                                                                                                            | Specifies the destination for a tunnel.<br><br>You must enter the MPLS traffic engineering router ID of the destination device.                                                                                                                                                   |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                                                                                                                        | Sets the tunnel encapsulation mode to MPLS traffic engineering.                                                                                                                                                                                                                   |
| Step 7 | <b>tunnel mpls traffic-eng bandwidth</b> <i>bandwidth</i><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng bandwidth 300                                                                                                                         | Configures the bandwidth required for the MPLS traffic engineering tunnel.                                                                                                                                                                                                        |
| Step 8 | <b>tunnel mpls traffic-eng path-option</b> <i>number</i> <b>explicit</b> { <i>name path-name</i>   <i>identifier path-number</i> } [ <b>lockdown</b> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name path-Tunnell | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.<br><br>The <b>name</b> keyword must specify the ABRs the tunnel LSP must traverse as loose hops via the <b>next-address loose</b> command. |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                                                                                                                                          | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                  |

## Configuring Explicit Paths

To configure explicit paths, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip explicit-path name *pathname***
4. **next-address [loose | strict] *ip-address***
5. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                              | Purpose                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                 | Enters global configuration mode.                                                                                                                   |
| Step 3 | <b>ip explicit-path name <i>pathname</i></b><br><br><b>Example:</b><br>Router(config)# ip explicit-path name path-tunnell                      | Enters IP explicit path configuration mode and creates or modifies the specified path.                                                              |
| Step 4 | <b>next-address [loose   strict] <i>ip-address</i></b><br><br><b>Example:</b><br>Router(config-ip-expl-path)# next-address loose 192.168.40.40 | Specifies the next IP address in the explicit path.<br><br>In a <b>next-address loose</b> command you must specify each ABR the path must traverse. |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-ip-expl-path)# end                                                                          | Returns to privileged EXEC mode.                                                                                                                    |

## Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination

To configure an MPLS traffic engineering tunnel with autoroute destination, perform the following steps.

### SUMMARY STEPS

1. **enable**



2. **configure terminal**
3. **interface** *tunnel-interface*
4. **ip unnumbered** *type number*
5. **tunnel destination** *ip-address*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** *bandwidth*
8. **tunnel mpls traffic-eng path-option** *number explicit* {**name** *path-name* | **identifier** *path-number*} [**lockdown**]
9. **tunnel mpls traffic-eng autoroute destination**
10. **end**

## DETAILED STEPS

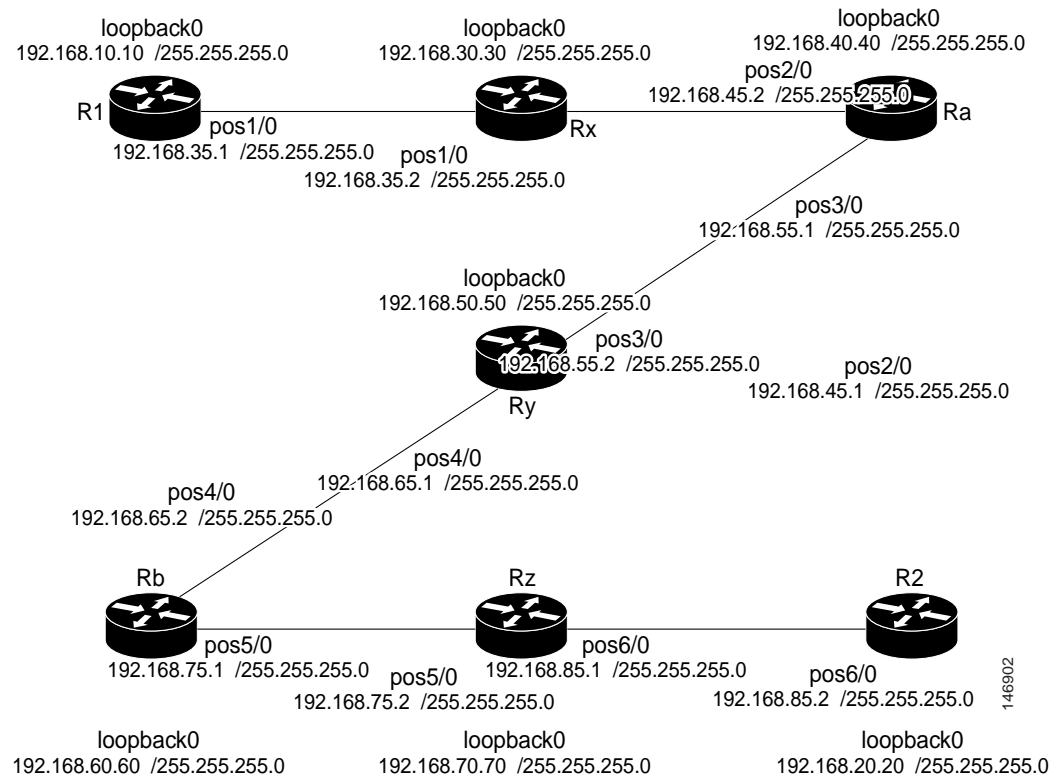
|        | Command or Action                                                                                                                            | Purpose                                                                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                               | Enters global configuration mode.                                                                                                                               |
| Step 3 | <b>interface</b> <i>tunnel-interface</i><br><br><b>Example:</b><br>Router(config)# interface Tunnel1                                         | Configures an interface type and enters interface configuration mode.                                                                                           |
| Step 4 | <b>ip unnumbered</b> <i>type number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered Loopback 0                                | Gives the tunnel interface an IP address.<br><br>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |
| Step 5 | <b>tunnel destination</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 192.168.20.20                    | Specifies the destination for a tunnel.<br><br>You must enter the MPLS traffic engineering router ID of the destination device.                                 |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                | Sets the tunnel encapsulation mode to MPLS traffic engineering.                                                                                                 |
| Step 7 | <b>tunnel mpls traffic-eng bandwidth</b> <i>bandwidth</i><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng bandwidth 300 | Configures the bandwidth required for the MPLS traffic engineering tunnel.                                                                                      |

|         | Command or Action                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <pre>tunnel mpls traffic-eng path-option <i>number</i> explicit {<i>name path-name</i>   <i>identifier</i> <i>path-number</i>} [<i>lockdown</i>]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>path-option 1 explicit name path-Tunnell</p> | <p>Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.</p> <p>The <b>name</b> keyword must specify the ABRs the tunnel LSP must traverse as loose hops via the <b>next-address loose</b> command.</p> |
| Step 9  | <pre>tunnel mpls traffic-eng autoroute <i>destination</i></pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng<br/>autoroute destination</p>                                                                                                           | Automatically routes traffic through a TE tunnel.                                                                                                                                                                                                                                        |
| Step 10 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                                                                                                                                                                          | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                         |

## Configuration Examples for MPLS Traffic Engineering: Interarea Tunnels

This section shows how to configure MPLS traffic engineering interarea tunnels for the simple router topology illustrated in [Figure 2](#). It includes configuration fragments that illustrate the configurations shown in the following sections:

- [Configuring OSPF for Interarea Tunnels: Example, page 19](#)
- [Configuring IS-IS for Interarea Tunnels: Example, page 20](#)
- [Configuring MPLS and RSVP to Support Traffic Engineering: Example, page 22](#)
- [Configuring an MPLS Traffic Engineering Interarea Tunnel: Example, page 22](#)
- [Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination: Example, page 23](#)

**Figure 2 Router Topology**

## Configuring OSPF for Interarea Tunnels: Example

The following configuration fragments show how to configure OSPF for interarea tunnels assuming that:

- Routers R1, Rx, and Ra are in OSPF Area 1
- Routers Ra, Ry, and Rb are in OSPF Area 0
- Routers Rb, Rz, and R2 are in OSPF Area 2
- Router Ra is an ABR for Area 0 and Area 1
- Router Rb is an ABR for Area 0 and Area 2

### Router R1 OSPF Configuration

```
router ospf 1
 network 192.168.10.10 0.0.0.0 area 1
 network 192.168.35.0 0.0.0.255 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
```

### Router Rx OSPF Configuration

```
router ospf 1
 network 192.168.30.30 0.0.0.0 area 1
 network 192.168.35.0 0.0.0.255 area 1
 network 192.168.45.0 0.0.0.255 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
```

**Router Ra OSPF Configuration**

Ra is an ABR for Area 0 and Area 1. Interface POS2/0 is in Area 1 and interface POS3/0 is in Area 0. The **mpls traffic-eng area** commands configure Ra for IGP TE updates for both areas.

```
router ospf 1
 network 192.168.40.40 0.0.0.0 area 0
 network 192.168.45.0 0.0.0.255 area 1
 network 192.168.55.0 0.0.0.255 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 1
```

**Router Rb OSPF Configuration**

Rb is an ABR for Area 0 and Area 2. Interface POS4/0 is in Area 0 and interface POS5/0 is in Area 2. The **mpls traffic-eng area** commands configure Rb for IGP TE updates for both areas.

```
router ospf 1
 network 192.168.60.60 0.0.0.0 area 0
 network 192.168.65.0 0.0.0.255 area 0
 network 192.168.75.0 0.0.0.255 area 2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
 mpls traffic-eng area 2
```

**Router Rz OSPF Configuration**

```
router ospf 1
 network 192.168.70.70 0.0.0.0 area 2
 network 192.168.75.0 0.0.0.255 area 2
 network 192.168.85.0 0.0.0.255 area 2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 2
```

**Router R2 OSPF Configuration**

```
router ospf 1
 network 192.168.20.20 0.0.0.0 area 2
 network 192.168.85.0 0.0.0.255 area 2
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 2
```

## Configuring IS-IS for Interarea Tunnels: Example

The following configuration fragments illustrate how to configure IS-IS for interarea tunnels assuming that:

- R1 and Rx are level-1 routers
- Ra, Ry, and Rb are level-1-2 routers
- Rz and R2 are level-1 routers

**Router R1 IS-IS Configuration**

```
interface POS1/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.0100.0000.0010
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
```

**Router Rx IS-IS Configuration**

```
clns routing
interface POS1/0
 ip router isis
interface POS2/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.2000.0100.0001
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
```

**Router Ra IS-IS Configuration**

```
clns routing
interface POS2/0
 ip router isis
interface POS3/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.2000.0200.0002
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
 mpls traffic-eng level-2
```

**Router Ry IS-IS Configuration**

```
clns routing
interface POS3/0
 ip router isis
interface POS4/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.2000.0300.0003
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
```

**Router Rb IS-IS Configuration**

```
clns routing
interface POS4/0
 ip router isis
interface POS5/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.2000.0400.0004
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-1
 mpls traffic-eng level-2
```

**Router Rz IS-IS Configuration**

```
clns routing
interface POS5/0
 ip router isis
interface POS6/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.2000.0500.0005
 mpls traffic-eng router-id Loopback0
```

```
mpls traffic-eng level-1
```

### Router R2 IS-IS Configuration

```
clns routing
interface POS6/0
 ip router isis
router isis
 metric-style wide
 net 10.0000.0200.0000.0020
mpls traffic-eng router-id Loopback0
mpls traffic-eng level-1
```

## Configuring MPLS and RSVP to Support Traffic Engineering: Example

The following configuration fragments show how to configure MPLS and RSVP to support traffic engineering on the routers.

### Router R1 Traffic Engineering Configuration

```
ip cef
mpls traffic-eng tunnels
interface Loopback0
 ip address 192.168.10.10 255.255.255.255
interface POS1/0
!Each interface supporting MPLS TE must include the following:
 mpls traffic-eng tunnels
 ip rsvp bandwidth
```

The configuration of routers Rx, Ra, Ry, Rb, Rz, and R2 for traffic engineering operation is similar to that for R1.

## Configuring an MPLS Traffic Engineering Interarea Tunnel: Example

The following configuration fragments show how to configure an MPLS traffic engineering interarea tunnel. Tunnel1 is configured with a path option that is loosely routed through Ra and Rb.

### R1 Interarea Tunnel Configuration

The following commands configure an MPLS TE tunnel to use explicit paths:

```
interface Tunnel1
 ip unnumbered Loopback0
 tunnel destination 192.168.20.20
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 300
 tunnel mpls traffic-eng path-option 1 explicit name path-tunnel1
```

The following commands configure an explicit path:

```
ip explicit-path name path-tunnel1
 next-address loose 192.168.40.40
 next-address loose 192.168.60.60
 next-address loose 192.168.20.20 !Specifying the tunnel tailend in the loosely routed
!path is optional.
```

**Note**

Generally for an interarea tunnel you should configure multiple loosely routed path options that specify different combinations of ABRs (for OSPF) or level-1-2 boundary routers (for IS-IS) to increase the likelihood that the tunnel will be successfully signaled. In this simple topology there are no other loosely routed paths.

## Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination: Example

The following example shows how to configure an MPLS TE tunnel with autoroute destination:

```
interface Tunnel103
 ip unnumbered Loopback0
 tunnel destination 10.1.0.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 1 explicit name 111-103
 tunnel mpls traffic-eng autoroute destination
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering: Interarea Tunnels feature.

## Related Documents

| Related Topic                     | Document Title                                                                                                                                                                      |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS                             | <ul style="list-style-type: none"><li><a href="#">Integrated IS-IS Routing Protocol Overview</a></li><li><a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li></ul> |
| Link protection                   | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a>                                                             |
| MPLS traffic engineering commands | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                                                                           |
| OSPF                              | <ul style="list-style-type: none"><li><a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li><li><a href="#">Configuring OSPF</a></li></ul>                           |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |



# Feature Information for MPLS Traffic Engineering: Interarea Tunnels

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering: Interarea Tunnels

| Feature Name                                | Releases                                                                                                                      | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering: Interarea Tunnels | 12.0(19)ST1<br>12.0(21)ST<br>12.2(18)S<br>12.2(18)SXD<br>12.2(27)SBC<br>12.2(28)SB<br>12.2(33)SRB<br>12.4(20)T<br>12.2(33)SRE | <p>The MPLS Traffic Engineering: Interarea Tunnels feature allows you to establish MPLS TE tunnels that span multiple IGP areas and levels, removing the restriction that had required the tunnel headend and tailend routers both to be in the same area.</p> <p>In 12.0(19)ST1, this feature was introduced.</p> <p>In 12.0(21)ST, support was added for the Cisco 10000 series routers.</p> <p>In 12.2(18)S, this feature was integrated.</p> <p>In 12.2(18)SXD, this feature was integrated.</p> <p>In 12.2(27)SBC, this feature was integrated.</p> <p>In 12.2(28)SB, this feature was integrated.</p> <p>In 12.2(33)SRB, support was added for stateful switchover (SSO) recovery of LSPs that include loose hops.</p> <p>In 12.4(20)T, support was eliminated for SSO recovery of LSPs that include loose hops.</p> <p>In 12.2(33)SRE, the autoroute destination feature was added. The following commands were added or modified: <b>show ip static route</b>, <b>show mpls traffic-eng autoroute</b>, <b>show mpls traffic-eng tunnels</b>, and <b>tunnel mpls traffic-eng autoroute destination</b>.</p> |

# Glossary

**ABR**—Area Border Router. A router connecting two areas. In OSPF, ABRs belong to both areas and must maintain separate topological databases for each. When an OSPF router has interfaces in more than one area, it is an Area Border Router.

**area**—A logical set of network segments (for example, one that is OSPF-based) and their attached devices. Areas usually are connected to other areas by routers, making up a single autonomous system. OSPF and IS-IS define their areas differently. OSPF area borders are marked by routers. Some interfaces are in one area, and other interfaces are in another area. With IS-IS, all the routers are completely within an area, and the area borders are on links, not on routers. The routers that connect the areas are level-2 routers, and routers that have no direct connectivity to another area are level-1 routers.

**area ID**—In an IS-IS router, this area address is associated with the entire router rather than an interface. A router can have up to three area addresses. Both the area ID and the system ID are defined on an IS-IS router by a single address, the Network Entry Title (NET).

**autonomous system**—A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas.

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks that have large and dynamic traffic patterns, such as the Internet, and for networks characterized by intensive Web-based applications or interactive sessions. Cisco Express Forwarding uses a Forwarding Information Base (FIB) to make IP destination prefix-based switching decisions. The FIB is conceptually similar to a routing table or information base. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains next-hop address information based on the information in the IP routing table.

**headend**—The upstream, transmit end of a tunnel. The router that originates and maintains the traffic engineering LSP.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include OSPF and Routing Information Protocol (RIP).

**interarea TE**—Ability for a traffic engineering LSP to span multiple areas.

**IS-IS**—Intermediate System-to-Intermediate System. IS-IS is an OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where intermediate system (IS) routers exchange routing information based on a single metric to determine the network topology.

**label switched path (LSP) tunnel**—A configured connection between two routers in which label switching is used to carry the packets.

**level-1 routers**—Routers that are directly connected to other areas. The routers are not in the backbone. MPLS does not run in the background. These routers are also called internal routers.

**level-2 routers**—Routers that connect two areas. These routers let you run MPLS in the background.

**load balancing**—The distribution of traffic among multiple paths to the same destination so that the router uses bandwidth efficiently. Load balancing increases the use of network segments, thus increasing effective network bandwidth.

**LSP**—label switched path. A sequence of hops such as R0...Rn in which a packet travels from R0 to Rn through label switching mechanisms. A label switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**mask**—A bit combination used to describe which part of an address refers to the network or the subnet and which part refers to the host.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**OSPF**—Open Shortest Path First. Link-state, hierarchical IGP routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

**process ID**—Distinguishes one process from another within the device. An OSPF process ID can be any positive integer, and it has no significance outside the router on which it is configured.

**router ID**—Something by which a router originating a packet can be uniquely distinguished from all other routers. For example, an IP address from one of the router's interfaces.

**static routing**—A static route is a fixed path preprogrammed by a network administrator. Static routes cannot make use of routing protocols and don't self-update after receipt of routing update messages; they must be updated by hand.

**tailend**—The downstream, receive end of a tunnel. The router that terminates the traffic engineering LSP.

**traffic engineering**—The techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**tunnel**—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

**virtual link**—Ordinarily, each area is directly connected to area 0. A virtual link is used for a connection when an area is connected to an area that is one area away from area 0.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2003–2009 Cisco Systems, Inc. All rights reserved.





# MPLS TE: Bundled Interface Support

---

**First Published: November 5, 2007**

**Last Updated: December 27, 2007**

The MPLS TE: Bundled Interface Support feature enables Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels over the bundled interfaces EtherChannel and Multilink PPP (MLP).

The Resource Reservation Protocol (RSVP) notifies TE about bandwidth changes that occur when member links are added or deleted, or when links become active or inactive. TE notifies other nodes in the network via IGP flooding. By default, the bandwidth available to TE LSPs is 75% of the interface bandwidth. You can change the percentage of the global bandwidth available for TE LSPs by using an RSVP command on the bundled interface. Bandwidth reservation and preemption are supported.

The Fast Reroute (FRR) feature is supported on the bundled interfaces. FRR is activated when a bundled interface goes down: for example, if you enter the **shut** command to shut down the interface, or fewer than the required minimum number of links are operational.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS TE: Bundled Interface Support](#)” section on [page 10](#).

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

- [Prerequisites for MPLS TE: Bundled Interface Support, page 2](#)
- [Restrictions for MPLS TE: Bundled Interface Support, page 2](#)



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Information About MPLS TE: Bundled Interface Support, page 2](#)
- [How to Configure MPLS TE: Bundled Interface Support, page 4](#)
- [Configuration Examples for MPLS TE: Bundled Interface Support, page 7](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)
- [Feature Information for MPLS TE: Bundled Interface Support, page 10](#)
- [Glossary, page 11](#)

## Prerequisites for MPLS TE: Bundled Interface Support

- Configure MPLS TE tunnels.
- Enable Cisco Express Forwarding in global configuration mode.
- Enable RSVP.
- Configure EtherChannel.
- Configure MLP.

## Restrictions for MPLS TE: Bundled Interface Support

- Traffic engineering over Service Virtual Interfaces (SVIs) is not supported unless the SVI consists of a bundle of links that represent a single point-to-point interface.
- There must be a valid IP address configuration on the bundled interface and there must not be an IP address configuration on the member links.
- To ensure that the Fast Reroute feature functions correctly in MLP, enter the **multilink min-links** command (to specify the preferred minimum number of links) along with the **mandatory** keyword (to deactivate the MLP bundle if the minimum number of links is not present).

## Information About MPLS TE: Bundled Interface Support

To configure the MPLS TE: Bundled Interface Support feature, you should understand the following concepts:

- [MLP Overview, page 2](#)
- [Cisco EtherChannel Overview, page 3](#)
- [Load Balancing and Min-Links in MLP and EtherChannel, page 4](#)

### MLP Overview

MLP provides the capability of splitting and recombining packets to a single end system across a logical pipe (also called a bundle) formed by multiple links. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP allows packets to be fragmented and the fragments to be sent at the same time over multiple point-to-point links to the same remote address. The multiple links come up in response to a dialer load threshold that you define. The load can be calculated on inbound traffic, outbound traffic, or on either, as needed for the traffic between the specific sites. MLP provides bandwidth on demand and reduces transmission latency across WAN links.

MLP is designed to work over single or multiple interfaces of the following types that are configured to support both dial-on-demand rotary groups and PPP encapsulation:

- Asynchronous serial interfaces
- Basic Rate Interfaces
- Primary Rate Interfaces

## Cisco EtherChannel Overview

Cisco EtherChannel technology builds upon standards-based 802.3 full-duplex Fast Ethernet to provide network managers with a reliable, high-speed solution for the campus network backbone. EtherChannel technology provides bandwidth scalability within the campus by providing up to 800 Mbps, 8 Gbps, or 80 Gbps of aggregate bandwidth for a Fast EtherChannel, Gigabit EtherChannel, or 10 Gigabit EtherChannel connection, respectively. Each of these connection speeds can vary in amounts equal to the speed of the links used (100 Mbps, 1 Gbps, or 10 Gbps). Even in the most bandwidth-demanding situations, EtherChannel technology helps aggregate traffic and keep oversubscription to a minimum, while providing effective link-resiliency mechanisms.

### Cisco EtherChannel Benefits

Cisco EtherChannel technology allows network managers to provide higher bandwidth among servers, routers, and switches than single-link Ethernet technology can provide.

Cisco EtherChannel technology provides incremental scalable bandwidth and the following benefits:

- **Standards-based**—Cisco EtherChannel technology builds upon IEEE 802.3-compliant Ethernet by grouping multiple, full-duplex point-to-point links. EtherChannel technology uses IEEE 802.3 mechanisms for full-duplex autonegotiation and autosensing, when applicable.
- **Flexible incremental bandwidth**—Cisco EtherChannel technology provides bandwidth aggregation in multiples of 100 Mbps, 1 Gbps, or 10 Gbps, depending on the speed of the aggregated links. For example, network managers can deploy EtherChannel technology that consists of pairs of full-duplex Fast Ethernet links to provide more than 400 Mbps between the wiring closet and the data center. In the data center, bandwidths of up to 800 Mbps can be provided between servers and the network backbone to provide large amounts of scalable incremental bandwidth.
- **Load balancing**—Cisco EtherChannel technology comprises several Fast Ethernet links and is capable of load balancing traffic across those links. Unicast, broadcast, and multicast traffic is evenly distributed across the links, providing improved performance and redundant parallel paths. When a link fails, traffic is redirected to the remaining links within the channel without user intervention and with minimal packet loss.
- **Resiliency and fast convergence**—When a link fails, Cisco EtherChannel technology provides automatic recovery by redistributing the load across the remaining links. When a link fails, Cisco EtherChannel technology redirects traffic from the failed link to the remaining links in less than one second. This convergence is transparent to the end user—no host protocol timers expire, so no sessions are dropped.

## Load Balancing and Min-Links in MLP and EtherChannel

Load balancing affects the actual and practical bandwidth that can be used for TE. Multilink load balancing uses a per-packet load balancing method. All of the bundle interface bandwidth is available. EtherChannel load balancing has various load balancing methods, depending on the traffic pattern and the load balancing configuration. The total bandwidth available for TE may be limited to the bandwidth of a single member link.

Min-links affects how FRR works. Multilink PPP Minimum Links (min-links) allows you to configure the minimum number of links in an MLP bundle required to keep that bundle active. To configure min-links for MLP, use the **multilink min-links** command. It is *recommended* that you specify the **mandatory** keyword. To use FRR, you *must* specify the **mandatory** keyword. On EtherChannel, min-link is supported only in the Link Aggregation Control Protocol (LACP). For other EtherChannel protocols, the minimum is one link, by default, and it is not configurable. To configure min-link for EtherChannel, use the **port-channel min-links** command.

## How to Configure MPLS TE: Bundled Interface Support

This section contains the following procedures:

- [Configuring MPLS TE on an MLP Interface, page 4](#) (required)
- [Configuring MPLS TE on an EtherChannel Interface, page 6](#) (required)

### Configuring MPLS TE on an MLP Interface

To configure MPLS TE on an MLP interface, perform the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask* [**secondary**]
5. **mpls traffic-eng tunnels**
6. **mpls traffic-eng backup-path** *tunnel*
7. **ppp multilink** [**ppp**]
8. **multilink min-links** *links* [**mandatory**]
9. **multilink-group** *group-number*
10. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
11. **keepalive** [*period* [*retries*]]
12. **end**



## DETAILED STEPS

|         | Command or Action                                                                                                               | Purpose                                                                                                                                                                                |
|---------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                       |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                  | Enters global configuration mode.                                                                                                                                                      |
| Step 3  | <b>interface type number [name-tag]</b><br><br><b>Example:</b><br>Router(config)# interface multilink 1                         | Creates a multilink bundle, assigns a group number to the bundle, and enters interface configuration mode.                                                                             |
| Step 4  | <b>ip address ip-address mask [secondary]</b><br><br><b>Example:</b><br>Router(config-if)# ip address 10.0.0.7 255.255.255.0    | Specifies an IP address for the multilink group.                                                                                                                                       |
| Step 5  | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng tunnels                           | Enables MPLS traffic engineering tunnel signaling on an interface (assuming that it is enabled on the device).                                                                         |
| Step 6  | <b>mpls traffic-eng backup-path tunnel</b><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng backup-path Tunnel50   | (Optional) Enables FRR.                                                                                                                                                                |
| Step 7  | <b>ppp multilink [ppp]</b><br><br><b>Example:</b><br>Router(config-if)# ppp multilink                                           | Enables MLP on an interface and, optionally, enables Bandwidth Allocation Control Protocol (BACP) and its Bandwidth Allocation Protocol (BAP) subset for dynamic bandwidth allocation. |
| Step 8  | <b>multilink min-links links [mandatory]</b><br><br><b>Example:</b><br>Router(config-if)# multilink min-links 2 mandatory       | Specifies the preferred minimum number of links in an MLP bundle.<br><br><b>Note</b> To use FRR, you must enter the <b>mandatory</b> keyword.                                          |
| Step 9  | <b>multilink-group group-number</b><br><br><b>Example:</b><br>Router(config-if)# multilink-group 1                              | Restricts a physical link to joining only a designated multilink-group interface.                                                                                                      |
| Step 10 | <b>ip rsvp bandwidth [interface-kbps] [single-flow-kbps]</b><br><br><b>Example:</b><br>Router(config-if)# ip rsvp bandwidth 100 | Enables RSVP for IP on an interface and specifies a percentage of the total interface bandwidth as available in the RSVP bandwidth pool.                                               |

|         | Command or Action                                                                                             | Purpose                                                                                                                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>keepalive</b> [ <i>period</i> [ <i>retries</i> ]]<br><br><b>Example:</b><br>Router(config-if)# keepalive 3 | Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface or before bringing the tunnel protocol down for a specific interface. |
| Step 12 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                   | Returns to global configuration mode.                                                                                                                                                                                                               |

## Configuring MPLS TE on an EtherChannel Interface

To configure MPLS TE on an EtherChannel interface, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip address** *ip-address mask* [**secondary**]
5. **mpls traffic-eng tunnels**
6. **mpls traffic-eng backup-path** *tunnel*
7. **port-channel min-links** *min-num*
8. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                           | Purpose                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                              | Enters global configuration mode.                                                                                                        |
| Step 3 | <b>interface type number [name-tag]</b><br><br><b>Example:</b><br>Router(config)# interface port-channel 1                                  | Creates an EtherChannel bundle, assigns a group number to the bundle, and enters interface configuration mode.                           |
| Step 4 | <b>ip address ip-address mask [secondary]</b><br><br><b>Example:</b><br>Router(config-if)# ip address 10.0.0.4 255.255.255.0                | Specifies an IP address for the EtherChannel group.                                                                                      |
| Step 5 | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng tunnels                                       | Enables MPLS TE tunnel signaling on an interface (assuming that it is enabled on the device).                                            |
| Step 6 | <b>mpls traffic-eng backup-path tunnel</b><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng backup-path Tunnel120              | (Optional) Enables FRR.                                                                                                                  |
| Step 7 | <b>port-channel min-links min-num</b><br><br><b>Example:</b><br>Router(config-if)# port-channel min-links 2                                 | Specifies that a minimum number of bundled ports in an EtherChannel is required before the channel can be active.                        |
| Step 8 | <b>ip rsvp bandwidth [interface-kbps]</b><br>[ <i>single-flow-kbps</i> ]<br><br><b>Example:</b><br>Router(config-if)# ip rsvp bandwidth 100 | Enables RSVP for IP on an interface and specifies a percentage of the total interface bandwidth as available in the RSVP bandwidth pool. |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                 | Returns to global configuration mode.                                                                                                    |

## Configuration Examples for MPLS TE: Bundled Interface Support

This section contains the following configuration examples:

- [Configuring MPLS TE on an MLP Interface: Example, page 8](#)
- [Configuring MPLS TE on an EtherChannel Interface: Example, page 8](#)

## Configuring MPLS TE on an MLP Interface: Example

The following example shows how to configure MPLS TE on an MLP interface:

```
interface multilink 1
ip address 10.0.0.7 255.255.255.0
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel50
ppp multilink
multilink min-links 2 mandatory
multilink-group 1
ip rsvp bandwidth 100
keepalive 3
```

## Configuring MPLS TE on an EtherChannel Interface: Example

The following example shows how to configure MPLS TE on an EtherChannel interface:

```
interface port-channel 1
ip address 10.0.0.4 255.255.255.0
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel120
port-channel min-links 2
ip rsvp bandwidth 100
```

## Additional References

The following sections provide references related to the MPLS TE: Bundled Interface Support feature.

## Related Documents

| Related Topic               | Document Title                            |
|-----------------------------|-------------------------------------------|
| Configuring EtherChannel    | <a href="#">Configuring EtherChannels</a> |
| EtherChannel Load Balancing | <a href="#">Configuring EtherChannels</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

This feature uses no new or modified commands.

# Feature Information for MPLS TE: Bundled Interface Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS TE: Bundled Interface Support

| Feature Name                       | Releases    | Feature Information                                                                                                                                                                                      |
|------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS TE: Bundled Interface Support | 12.2(33)SRC | The MPLS TE: Bundled Interface Support feature enables MPLS traffic engineering (TE) tunnels over the bundled interfaces EtherChannel and Multilink MLP.<br>In 12.2(33)SRC, this feature was introduced. |

# Glossary

**bundle**—A group of interfaces that comprise an aggregate interface; for example, MLP and EtherChannel.

**Cisco Express Forwarding**—A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**EtherChannel**—EtherChannel is a trunking technology that groups multiple full-duplex 802.3 Ethernet interfaces to provide fault-tolerant high-speed links between switches, routers, and servers. EtherChannel is a logical aggregation of multiple Ethernet interfaces. EtherChannel forms a single higher bandwidth routing or bridging endpoint.

**Fast EtherChannel**—Fast EtherChannel is a technology-leveraging, standards-based Fast Ethernet that provides the additional bandwidth network backbones require today. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers. It supports up to eight links per channel.

**Gigabit EtherChannel**—Gigabit EtherChannel is high-performance Ethernet technology that provides gigabit per second transmission rates. It provides flexible, scalable bandwidth with resiliency and load sharing across links for switches, router interfaces, and servers. It supports up to eight links per channel.

**member link**—An interface that is part of a bundle.

**min-links**—Minimum number of links in an MLP bundle.

**MLP**—Multilink PPP provides load balancing functionality over multiple WAN links, while providing multivendor interoperability, packet fragmentation, proper sequencing, and load calculation on both inbound and outbound traffic.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**PPP**—Point-to-Point Protocol. A successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. PPP was designed to work with several network layer protocols (such as IP, IPX, and ARA). PPP also has built-in security mechanisms (such as CHAP and PAP). PPP relies on two protocols: LCP and NCP.

**RSVP**—Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. Also known as Resource Reservation Setup Protocol.

**traffic engineering**—Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

---

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

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

---

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

© 2007 Cisco Systems, Inc. All rights reserved.

---





# MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels

---

**First Published: February 28, 2006**

**Last Updated: October 21, 2009**

The MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels feature provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load. The configured bandwidth in the running configuration is changed due to the automatic bandwidth behavior.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels” section on page 19](#).

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

## Contents

- [Prerequisites for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels, page 2](#)
- [Restrictions for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels, page 2](#)
- [Information About MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels, page 2](#)
- [How to Configure MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels, page 3](#)
- [Configuration Examples for MPLS TE—Automatic Bandwidth Adjustments for TE Tunnels, page 15](#)



---

**Americas Headquarters:**

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

- [Additional References, page 17](#)
- [Feature Information for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels, page 19](#)

## Prerequisites for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

Your network must support the following:

- Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels
- Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

MPLS TE must be configured on the interface and on the tunnels.

## Restrictions for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

- The automatic bandwidth adjustment feature treats each tunnel for which it has been enabled independently. That is, it adjusts the bandwidth for each such tunnel according to the adjustment frequency configured for the tunnel and the sampled output rate for the tunnel since the last adjustment without regard for any adjustments previously made or pending for other tunnels.
- If a tunnel is brought down to calculate a new label switched path (LSP) because the LSP is not operational, the configured bandwidth is not saved. If the router is reloaded, the last saved automatic bandwidth value is used.
- You cannot configure MPLS TE over the logical generic routing encapsulation (GRE) tunnel interface.

## Information About MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

Before you configure the MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels feature, you should understand the following:

- [MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels Overview, page 2](#)
- [MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels Benefits, page 3](#)

## MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels Overview

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, the feature periodically (for example, once per day) adjusts the tunnel's allocated bandwidth to be the largest sample for the tunnel since the last adjustment.

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

## MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels Benefits

The automatic bandwidth feature allows you to configure and monitor the bandwidth for MPLS TE tunnels. If automatic bandwidth is configured for a tunnel, TE automatically adjusts the tunnel's bandwidth.

# How to Configure MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

This section contains the following tasks to configure MPLS TE automatic bandwidth adjustment for TE tunnels:

- [Configuring a Device to Support Traffic Engineering Tunnels, page 3](#) (required)
- [Configuring IS-IS or OSPF for MPLS Traffic Engineering, page 4](#) (required)
- [Configuring Bandwidth on Each Link That a Tunnel Crosses, page 6](#) (required)
- [Configuring Bandwidth on Each Link That a Tunnel Crosses, page 6](#) (required)
- [Enabling Automatic Bandwidth Adjustment on a Platform, page 10](#) (required)
- [Enabling Automatic Bandwidth Adjustment for a Tunnel, page 11](#) (required)
- [Configuring the Interval for Computing the Tunnel Average Output Rate, page 12](#) (optional)
- [Verifying Automatic Bandwidth Configuration, page 13](#) (optional)

## Configuring a Device to Support Traffic Engineering Tunnels

To configure a device to support TE tunnels, perform the following task.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip cef distributed`
4. `mpls traffic-eng tunnels`
5. `exit`

**DETAILED STEPS**

|               | Command or Action                                                                                  | Purpose                                                                                                           |
|---------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                 |
| <b>Step 3</b> | <b>ip cef distributed</b><br><br><b>Example:</b><br>Router(config)# ip cef distributed             | Enables distributed Cisco Express Forwarding operation.                                                           |
| <b>Step 4</b> | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng tunnels | Enables the MPLS traffic engineering tunnel feature on a device.                                                  |
| <b>Step 5</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                         | Exits to privileged EXEC mode.                                                                                    |

**Configuring IS-IS or OSPF for MPLS Traffic Engineering**

Perform one of the follow tasks to configure IS-IS or OSPF for MPLS TE:

- [Configuring IS-IS for MPLS Traffic Engineering, page 4](#) (optional)
- [Configuring OSPF for MPLS Traffic Engineering, page 5](#) (optional)

**Configuring IS-IS for MPLS Traffic Engineering**

To configure IS-IS for MPLS TE, perform the following task.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router isis**
4. **mpls traffic-eng level-1**
5. **mpls traffic-eng router-id loopback0**
6. **metric-style wide**
7. **exit**
8. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                 |
| Step 3 | <b>router isis</b><br><br><b>Example:</b><br>Router(config)# router isis                                                          | Enables IS-IS routing and specifies an IS-IS process for IP, and enters router configuration mode.                |
| Step 4 | <b>mpls traffic-eng level-1</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng level-1                         | Turns on MPLS TE for IS-IS level 1.                                                                               |
| Step 5 | <b>mpls traffic-eng router-id loopback0</b><br><br><b>Example:</b><br>Router(config-router)# mpls traffic-eng router-id loopback0 | Specifies that the TE router identifier for the node is the IP address associated with interface loopback0.       |
| Step 6 | <b>metric-style wide</b><br><br><b>Example:</b><br>Router(config-router)# metric-style wide                                       | Configures a router to generate and accept only new-style type, length, value objects (TLVs).                     |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                 | Exits to global configuration mode.                                                                               |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                        | Exits to privileged EXEC mode.                                                                                    |

## Configuring OSPF for MPLS Traffic Engineering

To configure OSPF for MPLS TE, perform the following task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf process-id**

4. `mpls traffic-eng area number`
5. `mpls traffic-eng router-id loopback0`
6. `exit`
7. `exit`

## DETAILED STEPS

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                        |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <code>router ospf <i>process-id</i></code><br><br><b>Example:</b><br>Router(config)# <code>router ospf 200</code>                                    | Configures an OSPF routing process for IP and enters router configuration mode. <ul style="list-style-type: none"> <li>The value for the <i>process-id</i> argument is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process.</li> </ul> |
| Step 4 | <code>mpls traffic-eng area <i>number</i></code><br><br><b>Example:</b><br>Router(config-router)# <code>mpls traffic-eng area 0</code>               | Turns on MPLS TE for the indicated OSPF area.                                                                                                                                                                                                                                                                                                                           |
| Step 5 | <code>mpls traffic-eng router-id loopback0</code><br><br><b>Example:</b><br>Router(config-router)# <code>mpls traffic-eng router-id loopback0</code> | Specifies that the TE router identifier for the node is the IP address associated with interface loopback0.                                                                                                                                                                                                                                                             |
| Step 6 | <code>exit</code><br><br><b>Example:</b><br>Router(config-router)# <code>exit</code>                                                                 | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                     |
| Step 7 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# <code>exit</code>                                                                        | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                          |

## Configuring Bandwidth on Each Link That a Tunnel Crosses

To configure bandwidth on each link that a tunnel crosses, perform the following task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **mpls traffic-eng tunnels**
5. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*] [**sub-pool** *kbps*]
6. **exit**
7. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                    | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface FastEthernet 0/0/0                                                                                | Configures an interface type and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng tunnels                                                                                     | Enables MPLS TE tunnels on an interface.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 5 | <b>ip rsvp bandwidth</b> [ <i>interface-kbps</i> ]<br>[ <i>single-flow-kbps</i> ] [ <b>sub-pool</b> <i>kbps</i> ]<br><br><b>Example:</b><br>Router(config-if)# ip rsvp bandwidth 1000 100 | Enables Resource Reservation Protocol (RSVP) for IP on an interface.<br><ul style="list-style-type: none"> <li>The <i>interface-kbps</i> argument specifies the maximum amount of bandwidth (in kbps) that may be allocated by RSVP flows. The range is from 1 to 10000000.</li> <li>The <i>single-flow-kbps</i> argument is the maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10000000.</li> </ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                             | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Configuring an MPLS Traffic Engineering Tunnel

To configure an MPLS TE tunnel, perform the following task. The MPLS TE tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

**Note** The configuration applies only to the TE head-end node. The configuration applies to all nodes and interfaces in the network.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *interface-type interface-number*
5. **tunnel destination** *ip-address*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** *bandwidth*
8. **tunnel mpls traffic-eng path-option** [**protect**] *preference-number* {**dynamic** | **explicit** | {**name** *path-name* | *path-number*}} [**lockdown**]
9. **exit**
10. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                | Configures a tunnel interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>ip unnumbered</b> <i>interface-type interface-number</i><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 0 | Gives the tunnel interface an IP address that is the same as that of interface Loopback0.<br><ul style="list-style-type: none"> <li>• An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link.</li> </ul> <p><b>Note</b> This command is not effective until Loopback0 has been configured with an IP address.</p> |



|         | Command or Action                                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5  | <code>tunnel destination ip-address</code><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.3.3.3                                                                                                                                             | Specifies the destination for a tunnel. <ul style="list-style-type: none"> <li>The destination must be the MPLS TE router ID of the destination device.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6  | <code>tunnel mode mpls traffic-eng</code><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                                                                                                             | Sets the encapsulation mode of the tunnel to MPLS TE.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 7  | <code>tunnel mpls traffic-eng bandwidth bandwidth</code><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng bandwidth 250                                                                                                                     | Configures the bandwidth for the MPLS TE tunnel. <ul style="list-style-type: none"> <li>The <i>bandwidth</i> argument is the bandwidth, in kilobits per second, set for the MPLS TE tunnel. The range is from 1 to 4294967295. The default is 0.</li> <li>If automatic bandwidth is configured for the tunnel, the <b>tunnel mpls traffic-eng bandwidth</b> command configures the initial tunnel bandwidth, which will be adjusted by the autobandwidth mechanism.</li> </ul> <b>Note</b> If you configure a tunnel's bandwidth with the <b>tunnel mpls traffic-eng bandwidth</b> command and the minimum amount of automatic bandwidth with the <b>tunnel mpls traffic-eng auto-bw</b> command, the minimum amount of automatic bandwidth adjustment is the lower of those two configured values. |
| Step 8  | <code>tunnel mpls traffic-eng path-option [protect] preference-number {dynamic   explicit   {name path-name   path-number}} [lockdown]</code><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the TE topology database. <ul style="list-style-type: none"> <li>A dynamic path is used if an explicit path is currently unavailable.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 9  | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                                             | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 10 | <code>exit</code><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                                | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Troubleshooting Tips

Each **tunnel mpls traffic-eng auto-bw** command supersedes the previous one. Therefore, if you want to specify multiple options for a tunnel, you must specify them all in a single **tunnel mpls traffic-eng auto-bw** command.

## Enabling Automatic Bandwidth Adjustment on a Platform

To enable automatic bandwidth adjustment on a platform and initiate sampling the output rate for tunnels configured for bandwidth adjustment, perform the following task.

**Note** This task is applicable only to the TE head-end router. The configuration applies to all locally-configured TE head-end interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-bw timers [frequency *seconds*]**
4. **no mpls traffic-eng auto-bw timers**
5. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                    | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>mpls traffic-eng auto-bw timers [frequency <i>seconds</i>]</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-bw timers frequency 300 | Enables automatic bandwidth adjustment on a platform and begins sampling the output rate for tunnels that have been configured for automatic bandwidth adjustment.<br><ul style="list-style-type: none"> <li>The <b>frequency</b> keyword specifies the interval, in seconds, for sampling the output rate of each tunnel configured for automatic bandwidth. The range is 1 through 604800. The recommended value is 300.</li> </ul> |

|        | Command or Action                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><code>no mpls traffic-eng auto-bw timers</code></p> <p><b>Example:</b><br/> Router(config)# no mpls traffic-eng auto-bw timers</p> | <p>(Optional) Disables automatic bandwidth adjustment on a platform.</p> <ul style="list-style-type: none"> <li>Use the <b>no</b> version of the command, which terminates output rate sampling and bandwidth adjustment for tunnels. In addition, the <b>no</b> form of the command restores the configured bandwidth for each tunnel where the configured bandwidth is determined as follows: <ul style="list-style-type: none"> <li>If the tunnel bandwidth was explicitly configured via the <b>tunnel mpls traffic-eng bandwidth</b> command after the running configuration was written to the startup configuration, the configured bandwidth is the bandwidth specified by that command.</li> <li>Otherwise, the configured bandwidth is the bandwidth specified for the tunnel in the startup configuration.</li> </ul> </li> </ul> |
| Step 5 | <p><code>exit</code></p> <p><b>Example:</b><br/> Router(config)# exit</p>                                                             | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Enabling Automatic Bandwidth Adjustment for a Tunnel

To enable automatic bandwidth adjustment for a tunnel and constrain the range of automatic bandwidth adjustments applied to the tunnel, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **tunnel mpls traffic-eng auto-bw [collect-bw] [frequency *seconds*] [adjustment-threshold *percent*] [overflow-limit *number* overflow-threshold *percent*] [max-bw *kbps*] [min-bw *kbps*]**
5. **exit**
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                              | Enters global configuration mode.                                                                                              |
| Step 3 | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                                                                                                                                                                                                                                          | Configures a tunnel interface and enters interface configuration mode.                                                         |
| Step 4 | <b>tunnel mpls traffic-eng auto-bw</b> [ <i>collect-bw</i> ] [ <i>frequency seconds</i> ] [ <i>adjustment-threshold percent</i> ] [ <i>overflow-limit number</i> ] [ <i>overflow-threshold percent</i> ] [ <i>max-bw kbps</i> ] [ <i>min-bw kbps</i> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng auto-bw max-bw 2000 min-bw 1000 | Enables automatic bandwidth adjustment for the tunnel and controls the manner in which the bandwidth for a tunnel is adjusted. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                                                                                                                                               | Exits to global configuration mode.                                                                                            |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                                                                                                                                  | Exits to privileged EXEC mode.                                                                                                 |

## Configuring the Interval for Computing the Tunnel Average Output Rate

To specify the interval for computing the average output rate for an MPLS TE tunnel, perform the following task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **load-interval *seconds***
5. **exit**
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1 | Configures a tunnel interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                |
| Step 4 | <b>load-interval</b> <i>seconds</i><br><br><b>Example:</b><br>Router(config-if)# load-interval 90  | Configures the interval over which the input and output rates for the interface are averaged.<br><ul style="list-style-type: none"><li>The <i>seconds</i> argument is the length of time for which data is used to compute load statistics. The value is a multiple of 30, from 30 to 600 (30, 60, 90, 120, and so on). The default is 300.</li></ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                      | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                   |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                         | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                        |

## Verifying Automatic Bandwidth Configuration

To verify the automatic bandwidth configuration, perform the following task.

## SUMMARY STEPS

1. **show mpls traffic-eng tunnels**
2. **show running-config**

## DETAILED STEPS

**Step 1** **show mpls traffic-eng tunnels**

Use this command to display information about tunnels, including automatic bandwidth information for tunnels that have the feature enabled. For example:

```
Router# show mpls traffic-eng tunnels
```

```
Name:tagsw4500-9_t1 (Tunnel1) Destination:10.0.0.4
```

```

Status:
Admin:up Oper:up Path:valid Signalling:connected
path option 1, type explicit pbr_south (Basis for Setup, path weight 30)
path option 2, type dynamic
Config Parameters:
Bandwidth:13 kbps (Global) Priority:7 7 Affinity:0x0/0xFFFF
AutoRoute: disabled LockDown:disabled Loadshare:13 bw-based
auto-bw:(300/265) 53 Bandwidth Requested: 13
    Adjustment threshold: 5%
    Overflow Limit: 4 Overflow Threshold: 25%
    Overflow Threshold Crossed: 1
    Sample Missed: 1 Samples Collected: 1
Active Path Option Parameters:
    State: dynamic path option 1 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : Serial3/0, 18
RSVP Signalling Info:
    Src 10.0.0.1, Dst 10.0.0.4, Tun_Id 2, Tun_Instance 2
RSVP Path Info:
    My Address: 10.105.0.1
    Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
    Record Route: NONE
    Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
Record Route: NONE
    Tspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=13 kbits, burst=1000 bytes, peak rate=13 kbits
Shortest Unconstrained Path Info:
    Path Weight: 128 (TE)
    Explicit Route: 10.105.0.2 104.105.0.1 10.0.0.4
History:
Tunnel:
    Time since created: 7 minutes, 56 seconds
    Time since path change: 7 minutes, 18 seconds
    Number of LSP IDs (Tun_Instances) used: 2
    Number of Auto-bw Adjustment resize requests: 1
    Time since last Auto-bw Adjustment resize request: 1 minutes, 7 seconds
    Number of Auto-bw Overflow resize requests: 1
    Time since last Auto-bw Overflow resize request: 52 seconds
    Current LSP:
        Uptime: 52 seconds
        Selection: reoptimization
    Prior LSP:
ID: path option 1 [1]
Removal Trigger: configuration changed

```

In the command output:

- The auto-bw line indicates that automatic bandwidth adjustment is enabled for the tunnel.
- 300 is the time, in seconds, between bandwidth adjustments.
- 265 is the time, in seconds, remaining until the next bandwidth adjustment.
- 53 is the largest bandwidth sample since the last bandwidth adjustment.
- 13 is the last bandwidth adjustment and the bandwidth currently requested for the tunnel.
- The adjustment threshold is 5 percent.
- The overflow limit is 4.
- The overflow threshold is 25 percent.

- The overflow crossed is 1.

**Step 2 show running-config**

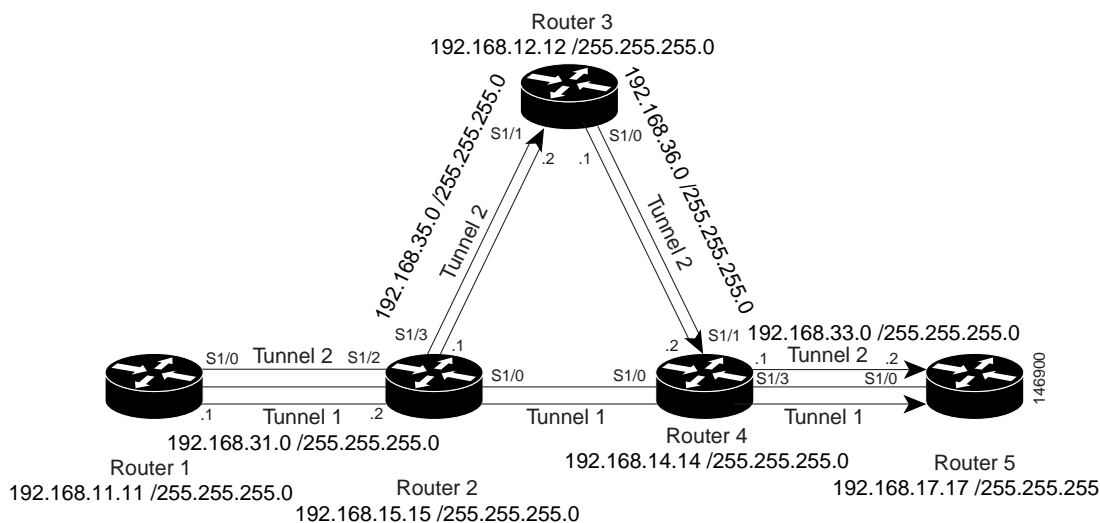
Use this command to verify that the **tunnel mpls traffic-eng auto bw** command is as you expected. For example:

```
Router# show running-config
.
.
.
interface tunnel1
  ip unnumbered loopback 0
  tunnel destination 192.168.17.17 255.255.255.0
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng bandwidth 1500
  tunnel mpls traffic-eng priority 1 1
  tunnel mpls traffic-eng path-option 1 dynamic
  tunnel mpls traffic-eng auto bw max-bw 2000 min-bw 1000    !Enable automatic bandwidth
.
.
.
```

The sample output from the **show running-config** command shows that the value 1500, in the **tunnel mpls traffic-eng bandwidth 1500** command, changes after an adjustment is made.

## Configuration Examples for MPLS TE—Automatic Bandwidth Adjustments for TE Tunnels

[Figure 1](#) illustrates a sample MPLS topology. The following sections contain sample configuration examples to configure automatic bandwidth adjustment for MPLS TE tunnels originating on Router 1 and to enable automatic bandwidth adjustment for Tunnel 1.

**Figure 1** Sample MPLS Traffic Engineering Tunnel Configuration

This section provides the following configuration examples based on [Figure 1](#):

- [Configuring MPLS Traffic Engineering Automatic Bandwidth: Example, page 16](#)
- [Tunnel Configuration for Automatic Bandwidth: Example, page 16](#)

The examples omit some configuration required for MPLS TE, such as the required RSVP and Interior Gateway Protocol (IGP) (IS-IS or OSPF) configuration, because the purpose of these examples is to illustrate the configuration for automatic bandwidth adjustment.

## Configuring MPLS Traffic Engineering Automatic Bandwidth: Example

The following example shows how to use the **mpls traffic-eng auto-bw timers** command to enable automatic bandwidth adjustment for Router 1. The command specifies that the output rate is to be sampled every 10 minutes for tunnels configured for automatic bandwidth adjustment.

```
configure terminal
!
ip cef distributed
mpls traffic-eng tunnels
mpls traffic-eng auto-bw timers frequency 600 !Enable automatic bandwidth adjustment
interface loopback 0
ip address 192.168.11.11 255.255.255.0
```

## Tunnel Configuration for Automatic Bandwidth: Example

The following example shows how to use the **tunnel mpls traffic-eng auto-bw** command to enable automatic bandwidth adjustment for Tunnel 1. The command specifies a maximum allowable bandwidth of 2000 kbps, a minimum allowable bandwidth of 1000 kbps, and that the default automatic bandwidth adjustment frequency of once a day be used.

```
interface tunnel1
ip unnumbered loopback 0
tunnel destination 192.168.17.17
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1500
tunnel mpls traffic-eng priority 1 1
```



```
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng auto-bw max-bw 2000 min-bw 1000    !Enable automatic bandwidth
   !adjustment for Tunnell
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—Automatic Bandwidth Adjustment for TE Tunnels feature.

### Related Documents

| Related Topic                              | Document Title                                                            |
|--------------------------------------------|---------------------------------------------------------------------------|
| IS-IS and OSPF commands                    | <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>          |
| MPLS commands                              | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |
| Quality of service solutions commands      | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>  |
| Quality of service solutions configuration | <a href="#">Quality of Service Overview</a>                               |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                          | MIBs Link                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                                                                                         | Title |
|-------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS TE—Automatic Bandwidth Adjustment for TE Tunnels

| Feature Name                                                                | Releases            | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels | Release 12.2(33)SRE | <p>The MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for TE Tunnels feature provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load. The configured bandwidth in the running configuration is changed due to the automatic bandwidth behavior.</p> <p>The following commands were introduced or modified to support automatic bandwidth adjustment threshold and overflow threshold: <b>mpls traffic-eng lsp attributes</b>, <b>show mpls traffic-eng tunnels</b>, and <b>tunnel mpls traffic-eng auto-bw</b>.</p> |

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2006–2009 Cisco Systems, Inc. All rights reserved.



# MPLS Point-to-Multipoint Traffic Engineering

---

**First Published: November 20, 2009**

**Last Updated: November 20, 2009**

The MPLS Point-to-Multipoint Traffic Engineering feature enables you to forward Multiprotocol Label Switching (MPLS) traffic from one source to multiple destinations.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS Point-to-Multipoint Traffic Engineering](#)” section on [page 34](#).

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

## Contents

- [Prerequisites for MPLS Point-to-Multipoint Traffic Engineering, page 2](#)
- [Restrictions for MPLS Point-to-Multipoint Traffic Engineering, page 2](#)
- [Information About MPLS Point-to-Multipoint Traffic Engineering, page 3](#)
- [How to Configure MPLS Point-to-Multipoint Traffic Engineering, page 13](#)
- [Configuration Examples for MPLS Point-to-Multipoint Traffic Engineering, page 24](#)
- [Additional References, page 30](#)
- [Glossary, page 31](#)
- [Feature Information for MPLS Point-to-Multipoint Traffic Engineering, page 34](#)



---

**Americas Headquarters:**

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

# Prerequisites for MPLS Point-to-Multipoint Traffic Engineering

Before configuring the MPLS Point-to-Multipoint Traffic Engineering (P2MP TE) feature, configure Resource Reservation Protocol (RSVP) and traffic engineering features on the headend, midpoint, and tailend routers in the MPLS network.

## Restrictions for MPLS Point-to-Multipoint Traffic Engineering

The following functionality is not supported:

- Interior Gateway Protocol (IGP) extensions for P2MP TE signaling, as defined in RFC 5073, are not supported.
- Multiple path options per destination are not supported. The P2MP TE feature allows one path option for each destination.
- P2MP TE is not supported in inter-area and autonomous system networks. All P2MP TE sub-label switched paths (LSPs) must originate and terminate in the same IGP and autonomous system domain.
- Path and node protection for P2MP sub-LSPs is not supported.
- The P2MP TE feature does not support nonstop forwarding/stateful switchover (NSF/SSO). However, NSF/SSO coexistence is supported.
- The P2MP TE feature does not support Protocol Independent Multicast (PIM) sparse mode. Only PIM source-specific multicast (SSM) is supported.
- The P2MP TE feature does not support dynamic adding and removal of destinations. You must manually add and remove destinations at the headend router.
- RFC 4090 describes two FRR methods: Facility and Detour backup. Both point-to-point (P2P) TE and P2MP TE support only the Facility FRR method.
- P2MP TE does not support the MIBs for P2MP tunnels as described in draft-ietf-mpls-p2mp-te-mib-09.txt. The P2MP TE headend interfaces are represented in the mplsTunnelTable of the MPLS-TE-STD-MIB. However, sub-LSP-related information is not supported by the MPLS-TE-STD-MIB.
- The MPLS LSP Ping and MPLS Operations, Administration, and Maintenance (OAM) features are not supported.
- P2MP TE does not support signaling of multiple sub-LSPs in the same Path/Resv message. If multiple sub-LSPs occur in the same message, the router sends a PathErr Unknown Objects message, and the Path/Resv message with multiple sub-LSPs is not forwarded.
- P2MP TE does not support RSVP local policies, which control the resources that RSVP reservations are allowed to use.
- P2MP TE does not support policy-based routing.
- P2MP TE cannot be configured with static IP routes.
- P2MP TE does not support penultimate-hop popping. Therefore, the egress router must allocate an explicit null or non-null label.
- The **tunnel mpls traffic-eng autoroute announce** command is not supported with this feature; it is supported only with IP unicast traffic.
- MPLS P2MP TE tunnels and IP Multicast (MFIB) do not support fragmentation. Configure MTU values on the ingress interface of the headend router.

- The following restrictions apply when port-channels are coupled with MPLS TE Fast Reroute:
  - Active and backup ports must be port-channel interfaces.
  - All members of the primary port-channel interfaces must be on the same slot.
  - All members of the backup port-channel must be on the same slot but different from the primary port-channel.

## Information About MPLS Point-to-Multipoint Traffic Engineering

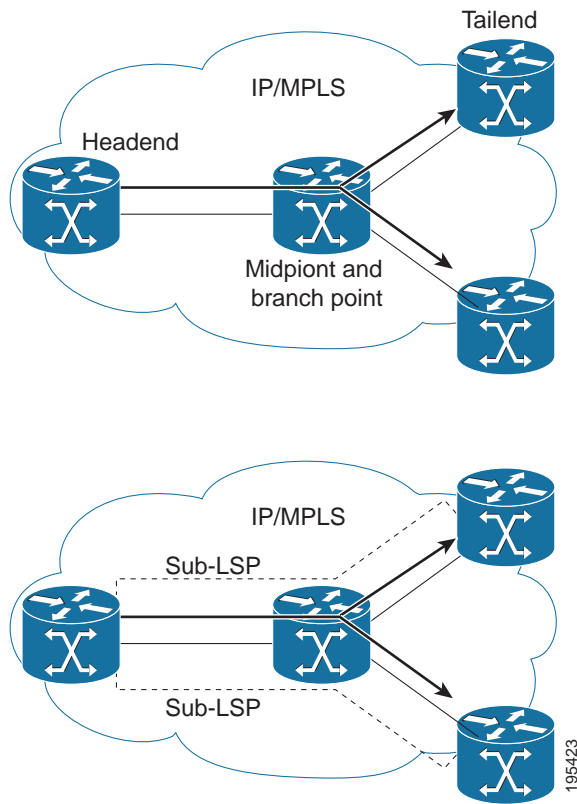
Before configuring the P2MP TE features, you should understand the following concepts:

- [MPLS Point-to-Multipoint Traffic Engineering Overview, page 3](#)
- [How P2MP TE Sub-LSPs Are Signaled, page 5](#)
- [How P2MP TE Traffic Is Forwarded, page 6](#)
- [Computing the IGP Path Using Dynamic Paths or Explicit Paths, page 7](#)
- [Benefits of MPLS Point-to-Multipoint Traffic Engineering, page 8](#)
- [MPLS Point-to-Multipoint Traffic Engineering—Re-optimizing Traffic, page 9](#)
- [P2P TE Tunnels Coexist with P2MP TE Tunnels, page 9](#)

## MPLS Point-to-Multipoint Traffic Engineering Overview

A P2MP TE network contains the following elements, which are shown in [Figure 1](#):

- The headend router, also called the source or ingress router, is where the label switched path (LSP) is initiated. The headend router can also be a branch point, which means the router performs packet replication and the sub-LSPs split into different directions.
- The midpoint router is where the sub-LSP signaling is processed. The midpoint router can be a branch point.
- The tailend router, also called the destination, egress, or leaf-node router, is where sub-LSP signaling ends.
- A bud router is a midpoint and tailend router at the same time.
- A P2MP tunnel consists of one or more sub-LSPs. All sub-LSPs belonging to the same P2MP tunnel employ the same constraints, protection policies, and so on, which are configured at the headend router.

**Figure 1 Basic P2MP TE Tunnels**

P2MP TE tunnels build on the features that exist in basic point-to-point TE tunnels. The P2MP TE tunnels have the following characteristics:

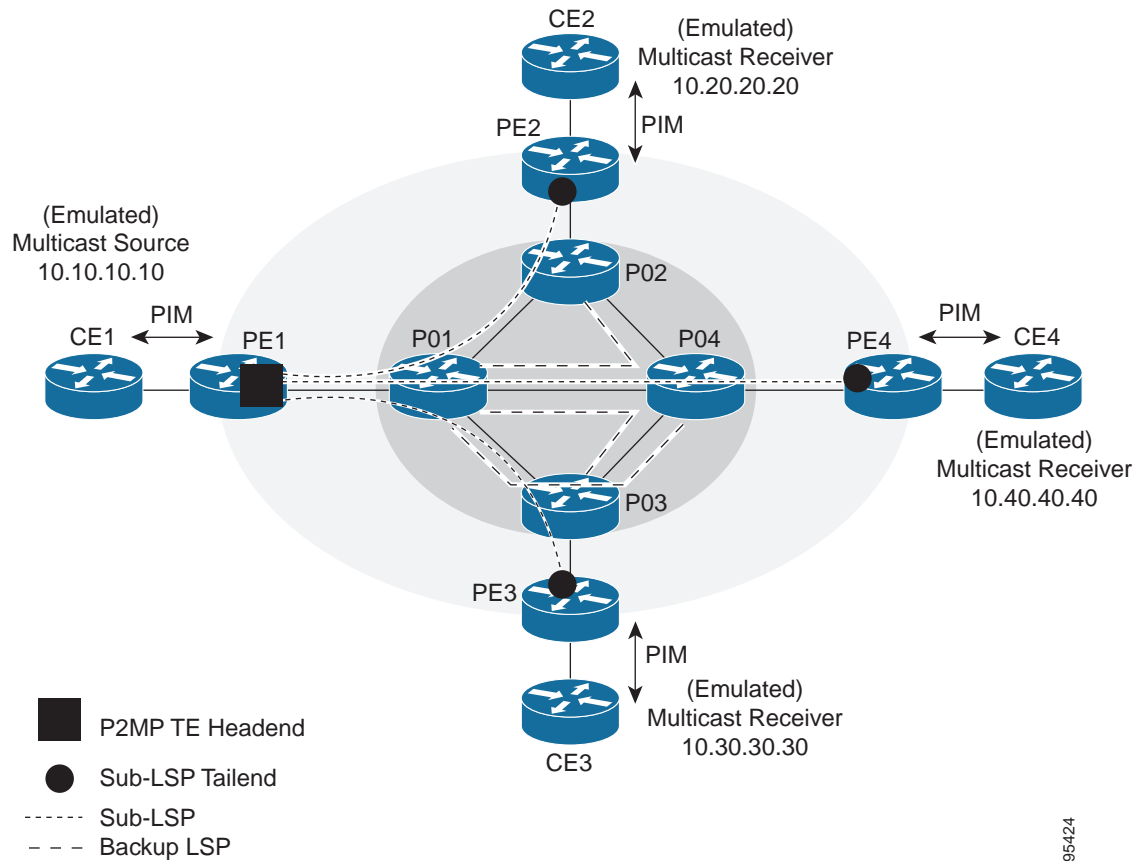
- There is one source (headend) but more than one destination (tailend).
- They are unidirectional.
- They are explicitly routed.
- Multiple sub-LSPs connect the headend router to various tailend routers.

Figure 2 shows a P2MP TE tunnel that has three destinations.

- PE1 is the headend router.
- P01 is a branch point router, where packet replication occurs.
- PE2, PE3, and PE4 are tailend routers, where the sub-LSP ends.

Between the PE and CE routers, PIM is enabled to exchange multicast routing information with the directly connected customer edge (CE) routers. PIM is not enabled across the P2MP TE tunnel.



**Figure 2** Network Topology with P2MP TE Tunnel

195424

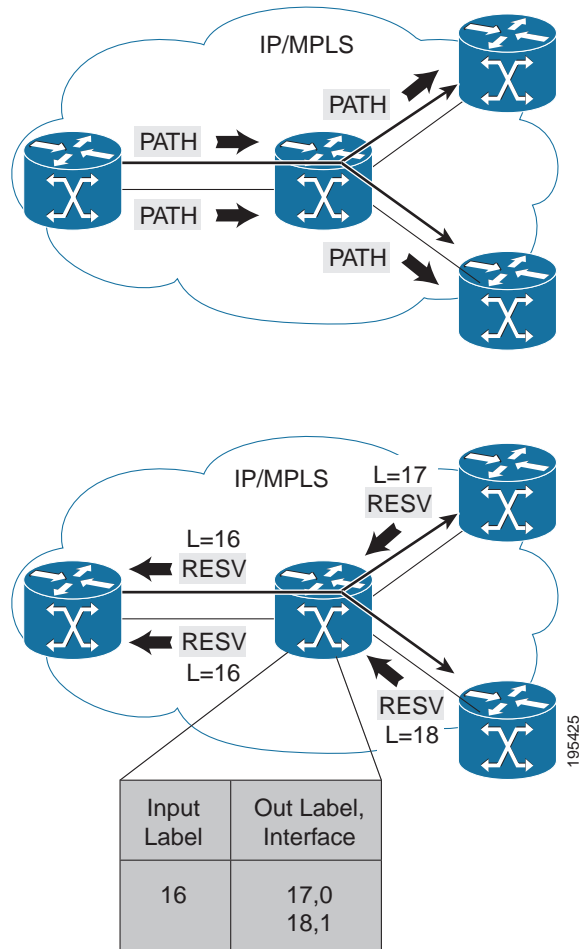
## How P2MP TE Sub-LSPs Are Signaled

RSVP TE extensions defined in RFC 4875 allow multiple sub-LSPs to be signaled from the headend router. A P2MP TE tunnel consists of multiple sub-LSPs that connect the headend router to various tailend routers.

The headend router sends one RSVP path message to each destination. The tailend router replies with a RESV message. The Label Forwarding Information Base (LFIB) is populated using the RSVP labels allocated by the RESV messages.

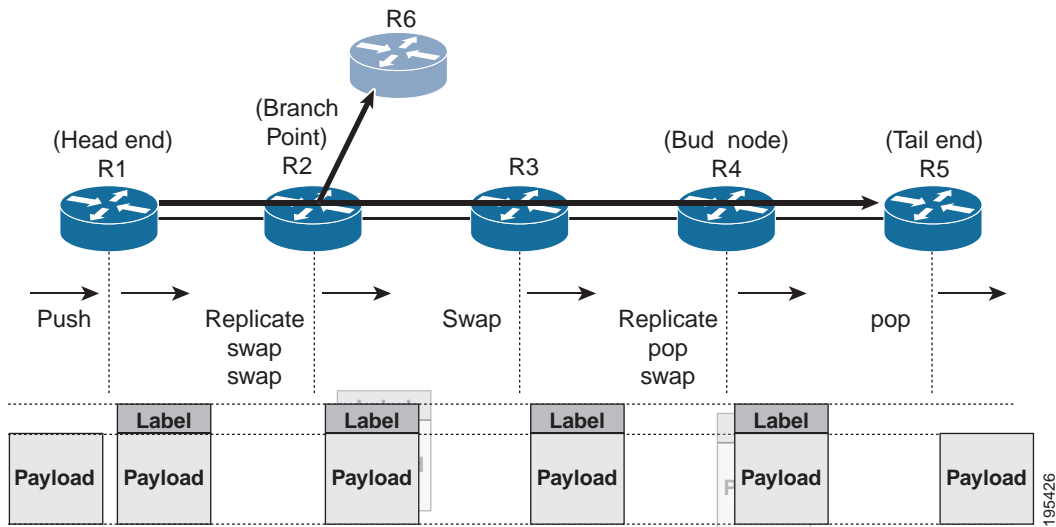
The tailend routers allocate unreserved labels, which are greater than 15 and do not include implicit or explicit null labels. Using unreserved labels allows IP Multicast to perform a Reverse Path Forwarding (RPF) check on the tailend router. Because a sub-LSP tailend router cannot be represented as a regular interface, a special LSP virtual interface (VIF) is automatically created. The LSP VIF represents the originating interface for all IP multicast traffic originating from the P2MP TE tailend router.

Figure 3 shows the LSP signaling process.

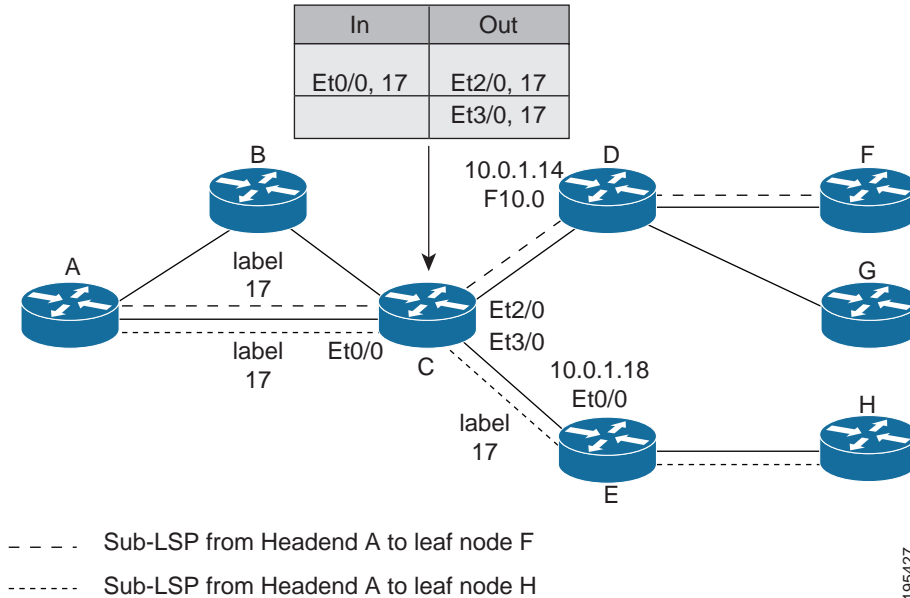
**Figure 3**      **How LSPs Are Signaled**

## How P2MP TE Traffic Is Forwarded

At the headend of the traffic engineering tunnel, through a static Internet Group Management Protocol (IGMP) group-to-tunnel mapping, IP multicast traffic is encapsulated with a unique MPLS label, which is associated with the P2MP TE tunnel. The multicast traffic is label switched in the P2MP tree and replicated at branch and bud nodes along the P2MP tree. When the labeled packet reaches the tailend (a PE router), the MPLS label is removed and forwarded to the IP multicast tree towards the end point. This process is shown in [Figure 4](#).

**Figure 4** How Packets Traverse the P2MP Tree

When sub-LSPs share a common router (branch point) and use the same ingress interface of the router, the same MPLS label is used for forwarding. The multicast state is built by reusing the MPLS labels at the branch points, as shown in Figure 5, where MPLS label 17 is shared by two sub-LSPs that both use router C.

**Figure 5** Reusing MPLS Labels in Branch Points

## Computing the IGP Path Using Dynamic Paths or Explicit Paths

You can either specify explicit paths or allow paths to be created dynamically. You can also specify bandwidth parameters, which are flooded throughout the MPLS network through existing RSVP-TE extensions to Open Shortest Path First (OSPF) and Integrated Intermediate System-to-Intermediate System (IS-IS).

The MPLS core network uses RSVP to enable end-to-end IP multicast connectivity. The tailend router and the end point router use PIM to exchange multicast routing information with directly connected CE routers. PIM is not configured in the MPLS core.

P2MP TE tunnels can co-exist with regular P2P TE tunnels. Existing path calculation and bandwidth preemption rules apply in this case.

You create IGP paths by enabling dynamic path computation, configuring explicit paths through CLI commands, or using both methods in your P2MP TE network.

- Dynamic paths are created using Constrained Shortest Path First (CSPF) to determine the best path to a destination. CSPF uses path constraints, such as bandwidth, affinities, priorities, and so on, as part of the computation.
- Explicit paths allows you to manually specify the path a sub-LSP uses from the headend router to the tailend router. You configure static paths on the headend router.

## Remerge Events

When explicit paths are configured with a limited number of equal cost links or paths, two sub-LSPs might connect at a midpoint router through different ingress interfaces, but use the same egress interface. This is called a remerge event, which can cause duplicate MPLS packets. If a router detects a remerge event, it sends a PathErr Routing Problem: Remerge Detected message toward the headend router and the sub-LSPs are not established. With dynamic paths, the router signals a path that avoids a remerge situation.

## Crossover Events

With a P2MP tunnel, two sibling sub-LSPs (sub-LSPs that share the same link and label) are said to “cross over” when they have different incoming interfaces and different outgoing interfaces on the same intersecting node. The sibling sub-LSPs neither share input label nor output bandwidth. Avoid configuring crossover LSPs, because they waste bandwidth. However, the duplication of sub-LSPs does not result in an error.

## Benefits of MPLS Point-to-Multipoint Traffic Engineering

The P2MP TE feature provides the following benefits:

- You can configure signaling attributes, such as affinities, administrative metrics, fast reroute protection, and bandwidth constraints, when you set up P2MP TE sub-LSPs.
- P2MP TE provides a single point of traffic control. You specify all the signaling and path parameters at the headend router.
- You can configure explicit paths to optimize traffic distribution.
- You can enable Fast Reroute link protection and bandwidth protection for P2MP TE sub-LSPs.
- Protocol Independent Multicast (PIM) is not needed in the MPLS core. Only the nonMPLS interfaces on the tailend routers need to be configured with PIM.

## MPLS Point-to-Multipoint Traffic Engineering—Re-optimizing Traffic

A P2MP TE tunnel is operational (up) when the first sub-LSP has been successfully signaled. The P2MP TE tunnel is not operational (down) when all sub-LSPs are down. Certain events can trigger a tunnel re-optimization:

- One of the sub-LSPs is fast-rerouted to a backup tunnel (for dynamic LSPs).
- A link is operational. (if the command **mpls traffic-eng reoptimize events link-up** is configured).
- A periodic, schedule optimization occurs through the **mpls traffic-eng reoptimize timers frequency** command.
- The network administrator forces a tunnel optimization through the **mpls traffic-eng reoptimize** command.
- A fast reroute protected interface becomes operational.
- A nonfast reroute LSP detects a remerge situation.

When a P2MP tunnel is reoptimized, a new LSP is signaled and traffic is moved to the new LSP.

To determine if a tunnel should be reoptimized, the router considers the following criteria:

- The router compares the number of reachable destinations between the new tree and current tree. If the new tree contains more reachable destinations than the current tree, the router performs a reoptimization. If the new tree contains fewer reachable destinations than the current tree, then the router keeps the current tree.
- The router verifies that the same set of reachable destinations in the current tree are also in the new tree. If the new tree does not contain the same destinations, the router keeps the current tree.
- The router compares the number of destinations in the new tree with the number of destinations in the old tree. If the number of destinations in the new tree is greater than the number of destinations in the current tree, the router switches to the new tree. This guarantees that the new tree will contain all of the existing destinations and more.
- The router compares the metric between the current and new tree to ensure the new tree and current tree contain the same set of reachable destinations.
- The router compares the administrative weights of the old tree and the new tree. The router switches to the new tree if the cumulative administrative weight is lower. This step applies as a tie breaker if all the other conditions are the same.

P2MP TE uses make-before-break reoptimization, which uses the following reoptimization process:

- The new LSP is signaled.
- The headend router initiates a timer to ensure sufficient time elapses before traffic moves from the current LSP to the new LSP.
- Traffic is redirected from the current LSP to the new LSP.
- The timer is started for the purpose of tearing down the old sub-LSPs.

## P2P TE Tunnels Coexist with P2MP TE Tunnels

Both P2P and P2MP TE tunnels share the following characteristics:

- Tunnel bandwidth is configured the same way in both P2P and P2MP tunnels. In P2MP TE tunnels, any bandwidth parameters you configure are applied to all the destination routers. That is, the bandwidth parameters apply to all sub-LSPs. Both P2P and P2MP TE tunnels use the same IGP extension to flood link bandwidth information throughout the network.
- Tunnel setup and hold priorities, attributes flags, affinity and mask, and administrative weight parameters are configured the same way for P2P and P2MP TE tunnels. P2MP TE tunnel parameters apply to all sub-LSPs.
- Fast Reroute-enabled P2MP sub-LSPs coexist with Fast Reroute-enabled P2P LSPs in a network. For P2P TE, node, link, and bandwidth protection is supported. For P2MP TE, only link and bandwidth protection are supported.
- The method of computing the path dynamically through CSPF is the same for P2P and P2MP TE.
- Auto-tunnel backup behaves slightly different with P2P and P2MP tunnels. With P2P tunnels, auto-tunnel backup creates two backup tunnels: one for the node protection and one for the link protection. The node protection backup is preferred for P2P LSP protection. With P2MP tunnels, auto-tunnel backup creates one backup tunnel, which is the link protection. Only the link protection backup can be used for P2MP sub-LSPs. The P2P and P2MP tunnels can coexist and be protected.

**Note**

If P2MP sub-LSPs are signaled from R1->R2->R3 and a P2P tunnel is signaled from R3->R2->R1, then issue the **mpls traffic-eng multicast-intact** command on R3 in IGP configuration mode under router OSPF or IS-IS to ensure to accommodate multicast traffic for R3's sub-LSPs.

## Using Fast Reroute to Protect P2MP TE Links

Fast Reroute applies to P2P LSPs and P2MP sub-LSPs in the same manner. No new protocol extensions are needed to support P2MP.

**Note**

For P2MP TE fast reroute protection, issue the **ip routing protocol purge interface** command on every penultimate hop router. Otherwise, the router can lose up to 6 seconds worth of traffic during a fast reroute cutover event.

Fast Reroute minimizes interruptions in traffic delivery as a result of link or node failure. FRR temporarily fast switches LSP traffic to a backup path around a network failure until the headend router signals a new end-to-end LSP.

Fast Reroute-enabled P2MP sub-LSPs coexist with Fast Reroute-enabled P2P LSPs in a network. For P2MP TE, only link and bandwidth protection is supported. Node, link, and bandwidth protection are supported for P2P TE.

You can configure P2P explicit backup tunnels on point of local repair (PLR) nodes for link protection of P2MP sub-LSPs, similar to LSPs for P2P TE tunnels. You can also enable automatic creation of backup tunnels using the Auto-tunnel Backup feature for P2P TE tunnels. All sibling sub-LSPs that share the same outgoing link are protected by the same backup tunnel. All cousin sub-LSPs that share the same outgoing link can be protected by multiple P2P backup tunnels.

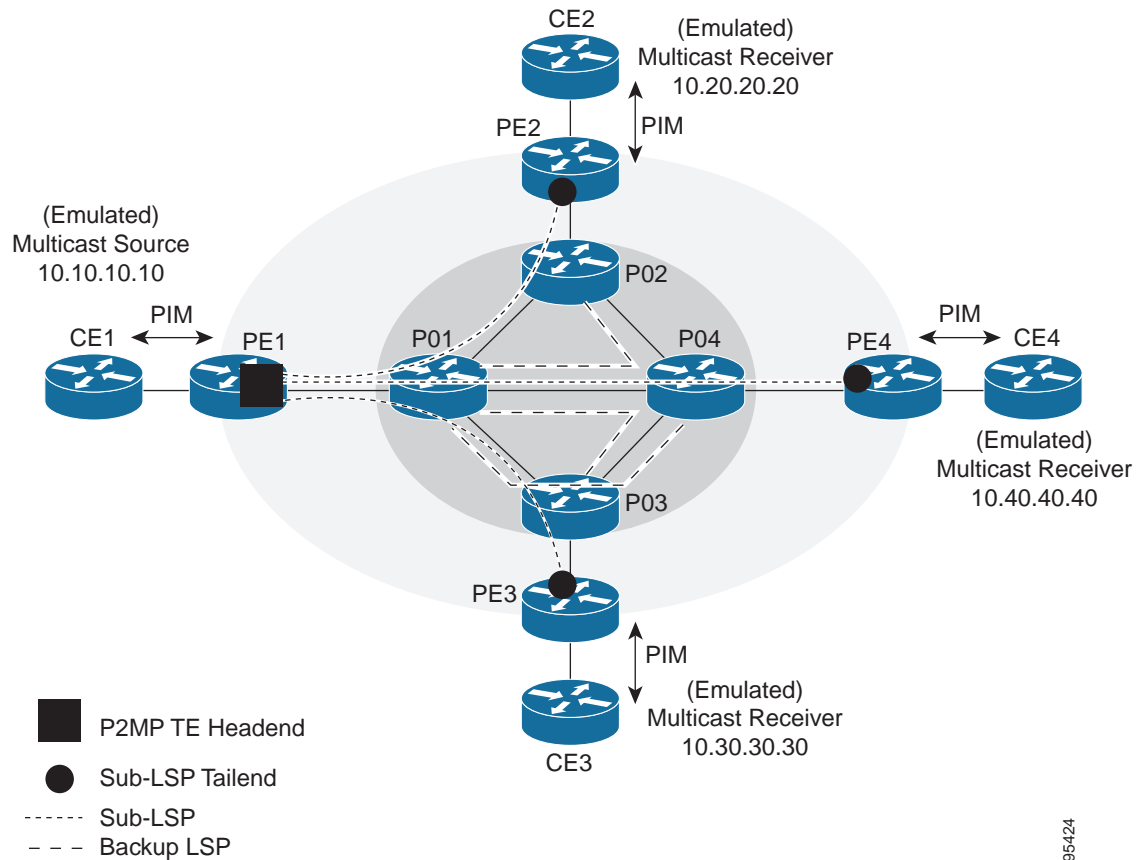
Link protection for a P2MP TE tunnel is illustrated in [Figure 6](#), which shows PE1 as the tunnel headend router and PE2, PE3, and PE4 as tunnel tailend routers. The following sub-LSPs are signaled from PE1 in the network:

- From PE1 to PE2, the sub-LSP travels the following path: PE1 -> P01 -> P02 -> PE2
- From PE1 to PE3, the sub-LSP travels the following path: PE1 -> P01 -> P03 -> PE3

- From PE1 to PE4, the sub-LSP travels the following path: PE1 -> P01 -> P04 -> PE4

Node P01 is a branch node that does packet replication in the MPLS forwarding plane; ingress traffic originating from PE1 will be replicated towards routers P02, P03, and P04.

**Figure 6 P2MP TE Link Protection Example**



To protect the three sub-LSPs, separate point-to-point backup tunnels are signaled. Note that backup tunnels can be created only for links that have an alternative network path. In this example, router P01 is the Point of Local Repair (PLR) and routers P02, P03, and P04 are Merge Points (MPs).

If a link failure occurs between routers P01 and P04, the following events are triggered:

- Router P01 switches traffic destined to PE4 to the backup tunnel associated with P04.
- Router P01 sends RSVP path error messages upstream to the P2MP TE headend router PE1. At the same time, P01 and P04 send IGP updates (link state advertisements (LSAs)) to all adjacent IGP neighbors, indicating that the interfaces associated with links P01 through P04 are down.
- Upon receiving RSVP path error messages and IGP LSA updates, the headend router triggers a P2MP TE tunnel reoptimization and signals a new sub-LSP. (This occurs if you have specified dynamic path creation.)



**Note**

If only one sub-LSP becomes active, it remains down until all the sub-LSPs become active.

## FRR Failure Detection Mechanisms

To detect link failures in a P2MP TE network, you can use native link and interface failure detection mechanisms, such as bidirectional forwarding detection (BFD), loss of signal (LoS) failure events, and RSVP hellos.

### Bidirectional Forwarding Detection

The MPLS Traffic Engineering: BFD-triggered Fast Reroute feature allows you to obtain link and node protection by using the Bidirectional Forwarding Detection (BFD) protocol to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. For more information, see [MPLS Traffic Engineering: BFD-triggered Fast Reroute \(FRR\)](#).

### Loss of Signal Failure Events

Fast Reroute can be triggered by loss of signal events. It is alarm based and dependent upon platform and line card support. For more information, see [MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#)

### RSVP Hellos

You can configure RSVP hellos on interfaces that do not provide FRR cutover notification during a link failure. The behavior for RSVP hellos is similar for both P2MP TE and P2P TE. For every sub-LSP that has a backup tunnel and has RSVP hellos enabled on its output interface, an RSVP hello instance is created to the neighbor, and the sub-LSP is added to the neighbor's FRR tree in the hello database.

Hello instances between an output interface and neighbor address are shared by fast reroutable P2MP sub-LSPs and P2P LSPs. When a hello session to a neighbor is declared down, all P2P LSPs and P2MP sub-LSPs that are protected by a backup LSP or sub-LSP are switched to their respective backups in the control and data planes.

RSVP hello sessions can also be used to inform the P2MP headend router of failures along a sub-LSP's path before the RSVP state for the sub-LSP times out, which leads to faster reoptimization. If a sub-LSP cannot select a backup tunnel but has RSVP hellos enabled on its output interface, it looks for a hello instance to its neighbor. If none exists, a hello state time (HST) hello instance is created. If the neighbor goes down, that sub-LSP is torn down. For more information, see [MPLS Traffic Engineering \(TE\) - Fast Reroute \(FRR\) Link and Node Protection](#).

## Bandwidth Preemption for P2MP TE

Bandwidth Admission Control and preemption mechanisms for P2MP TE sub-LSPs are the same as for LSPs associated with P2P TE tunnels. Any link affinities or constraints defined for the P2MP TE tunnel will be taken into account. The bandwidth signaled for the sub-LSP is removed from the appropriate pool at the appropriate priority, and if needed, lower priority sub-LSPs are preempted with a higher priority sub-LSP.

A P2MP tunnel can be configured to use sub-pool or global-pool bandwidth. When bandwidth is configured, all sub-LSPs of the P2MP tunnel are signaled with the same bandwidth amount and type. If the bandwidth amount or type of a P2MP tunnel is changed, the P2MP tunnel ingress always signals a new set of sub-LSPs (a new P2MP LSP) with the new bandwidth amount and type.

Preemption procedures do not take into account the tunnel type. The same priority rules apply to P2P LSPs and P2MP sub-LSPs. A sub-LSP with a higher setup priority preempts a (sub-)LSP with a lower hold priority, regardless of tunnel type. Thus, a P2MP sub-LSP may preempt a P2P LSP, and vice versa. The determination of which LSPs get preempted is based on hold priority.



You can configure a P2MP TE tunnel to use subpool or global-pool bandwidth. All sub-LSPs associated with the P2MP TE tunnel are signaled with the same bandwidth amount and type. If the bandwidth amount or type is changed, the P2MP tunnel headend router signals a new set of sub-LSPs with the new bandwidth parameters.

Bandwidth sharing is similar for P2MP TE sub-LSPs and P2P TE LSPs. When adding a new sub-LSP, the P2MP-TE headend router determines whether it should share bandwidth with the other sub-LSPs. Two sub-LSPs can share bandwidth as long as they are a “Transit Pair,” meaning the sub-LSPs share the output interface, next-hop and output label.

LSPs and sub-LSPs cannot share bandwidth if they use different bandwidth pools. A change in bandwidth requires reoptimizing P2P or P2MP TE tunnels, which may result in double-counting bandwidth on common links.

Using FRR with Bandwidth Protection has the following requirements:

- A backup tunnel is required to maintain the service level agreement while the new sub-LSP is created.
- The PLR router selects the backup tunnel only if the tunnel has enough bandwidth capacity.
- The backup tunnel might not signal bandwidth.
- The PLR router decides the best backup path to protect the primary path, based on backup bandwidth and class type.

## NSF/SSO Support for MPLS P2MP TE

NSF/SSO coexistence is supported with P2MP TE. State information associated with active P2MP tunnels and associated sub-LSPs is not checkpointed and cannot be recovered after a route processor (RP) failover. When a RP switchover is triggered through NSF/SSO, traffic going to P2MP TE tunnels is lost. P2MP TE sends RSVP path error messages upstream and RSVP RESV error messages downstream to tear down the affected P2MP sub-LSPs. The RSVP error message can also trigger a FRR switchover to backup paths, and the TE headend router can recalculate and resignal a new P2MP TE tunnel.

## How to Configure MPLS Point-to-Multipoint Traffic Engineering

Use the following procedures to configure the P2MP TE feature:

- [Configuring the Headend Routers, page 13](#) (required)
- [Configuring the Midpoint Routers, page 16](#) (required)
- [Configuring the Tailend Routers, page 17](#) (required)
- [Configuring Fast Reroute with P2MP TE Tunnels, page 19](#) (optional)
- [Enabling MPLS Traffic Engineering System Logging of Events, page 19](#) (optional)
- [Verifying the Configuration of MPLS Traffic Engineering Point-to-Multipoint Tunnels, page 19](#) (optional)

### Configuring the Headend Routers

The following steps explain how to configure the headend routers for Multicast and MPLS point-to-multipoint traffic engineering. As part of the configuration, you specify the tailend routers. You can also specify explicit paths that the tunnel should use or request that the paths be dynamically created or have a combination of dynamic and explicit paths.

Because the configuration of the P2MP TE tunnels is done at the headend router, this feature works best in situations where the destinations do not change often. The P2MP feature does not support dynamic grafting and pruning of sub-LSPs.

## Restrictions

- The **tunnel destination** command is not supported with point-to-multipoint traffic engineering tunnels. Instead, use the **mpls traffic-eng destination list** command.
- Multiple path options per sub-LSP (destination) are not supported. The P2MP TE feature allows one path option for each sub-LSP.
- The **tunnel mpls traffic-eng autoroute announce** command is not supported with this feature; it is supported only with IP unicast traffic.
- If P2MP sub-LSPs are signaled from R1->R2->R3 and a P2P tunnel is signaled from R3->R2->R1, then issue the **mpls traffic-eng multicast-intact** command on R3 in IGP configuration mode under router OSPF or IS-IS to ensure accommodate multicast traffic for R3's sub-LSPs.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng tunnels**
4. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
5. **interface tunnel** *number*
6. **tunnel mode mpls traffic-eng point-to-multipoint**
7. **tunnel destination list mpls traffic-eng** {**identifier** *dest-list-id* | **name** *dest-list-name*}
8. **ip igmp static-group** {**\*** | *group-address* [**source** {*source-address* | **ssm-map**}] | **class-map** *class-map-name*}
9. **ip pim** {**dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode**}
10. **exit**
11. **mpls traffic-eng destination list** {**name** *dest-list-name* | **identifier** *dest-list-id*}
12. **ip** *ip-address* **path-option** *id* {**dynamic** | **explicit** {**name** *name* | **identifier** *id*} [**verbatim**]}
13. **exit**
14. **ip explicit-path** {**name** *word* | **identifier** *number*} [**enable** | **disable**]
15. **next-address** [**loose** | **strict**] *ip-address*
16. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                        |
| Step 3 | <b>mpls traffic-eng tunnels</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng tunnels                                                                                                                                                                       | Globally enables MPLS Traffic Engineering. <ul style="list-style-type: none"> <li>Also issue this command on each network interface that supports a traffic engineering tunnel.</li> </ul>               |
| Step 4 | <b>ip multicast-routing</b> [vrf <i>vrf-name</i> ]<br>[ <i>distributed</i> ]<br><br><b>Example:</b><br>Router(config)# ip multicast-routing                                                                                                                              | Globally enables IP multicast routing.                                                                                                                                                                   |
| Step 5 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 100                                                                                                                                                                     | Configures a tunnel and enters interface configuration mode.                                                                                                                                             |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><b>point-to-multipoint</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng point-to-multipoint                                                                                                          | Enables MPLS point-to-multipoint traffic engineering on the tunnel.                                                                                                                                      |
| Step 7 | <b>tunnel destination list mpls traffic-eng</b><br>{ <i>identifier</i> <i>dest-list-id</i>   <i>name</i> <i>dest-list-name</i> }<br><br><b>Example:</b><br>Router(config-if)# tunnel destination list mpls traffic-eng name in-list-01                                   | Specifies a destination list to specify the IP addresses of point-to-multipoint destinations.                                                                                                            |
| Step 8 | <b>ip igmp static-group</b> { <i>*</i>   <i>group-address</i> [ <i>source</i> { <i>source-address</i>   <i>ssm-map</i> }]}   <b>class-map</b> <i>class-map-name</i><br><br><b>Example:</b><br>Router(config-if)# ip igmp static-group 239.100.100.101 source 10.11.11.11 | Configures static group membership entries on an interface. <ul style="list-style-type: none"> <li>Configure this on the TE tunnel interface if the source address (S, G) cannot be resolved.</li> </ul> |

|         | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <pre>ip pim {dense-mode [proxy-register {list access-list   route-map map-name}]   passive   sparse-mode   sparse-dense-mode}</pre> <p><b>Example:</b><br/>Router(config-if)# ip pim passive</p>   | <p>Enable Protocol Independent Multicast (PIM) on an interface.</p> <ul style="list-style-type: none"> <li>An interface configured with passive mode does not pass or forward PIM control plane traffic; it passes or forwards only IGMP traffic.</li> </ul>                                                                   |
| Step 10 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                                                                 | Exits interface configuration mode.                                                                                                                                                                                                                                                                                            |
| Step 11 | <pre>mpls traffic-eng destination list {name dest-list-name   identifier dest-list-id}</pre> <p><b>Example:</b><br/>Router(config)# mpls traffic-eng destination<br/>list name in-list-01</p>      | Creates a destination list and enters traffic engineering destination list configuration mode.                                                                                                                                                                                                                                 |
| Step 12 | <pre>ip ip-address path-option id {dynamic   explicit {name name   identifier id} [verbatim]}</pre> <p><b>Example:</b><br/>Router (cfg-te-dest-list)# ip 10.10.10.10<br/>path-option 1 dynamic</p> | <p>Specifies the IP addresses of MPLS point-to-multipoint traffic engineering tunnel destinations.</p> <ul style="list-style-type: none"> <li>If you use the <b>explicit</b> keyword, you must configure explicit paths, using the <b>ip explicit-path</b> command.</li> <li>Repeat this step for each destination.</li> </ul> |
| Step 13 | <pre>exit</pre> <p><b>Example:</b><br/>Router (cfg-te-dest-list)# exit</p>                                                                                                                         | Exits traffic engineering destination list configuration mode.                                                                                                                                                                                                                                                                 |
| Step 14 | <pre>ip explicit-path {name word   identifier number} [enable   disable]</pre> <p><b>Example:</b><br/>Router(config)# ip explicit-path name path1<br/>enable</p>                                   | Specifies the name of an IP explicit path and enters ip explicit path command mode command mode.                                                                                                                                                                                                                               |
| Step 15 | <pre>next-address [loose   strict] ip-address</pre> <p><b>Example:</b><br/>Router(cfg-ip-expl-path)# next-address 10.0.0.2</p>                                                                     | Specifies an explicit path that includes only the addresses specified or loose explicit paths.                                                                                                                                                                                                                                 |
| Step 16 | <pre>end</pre> <p><b>Example:</b><br/>Router(cfg-ip-expl-path)# end</p>                                                                                                                            | Exits the current configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                      |

## Configuring the Midpoint Routers

No special configuration is needed to support P2MP TE on the midpoint routers. The midpoint routers must have Cisco IOS Release 12.2(33)SRE or later release installed. They must be able to support and implement the P2MP signaling extensions. The MPLS TE configuration of the midpoint routers supports both P2P and P2MP TE. All multicast traffic is label switched. The midpoint routers do not require IPv4 multicast routing or PIM. For information on configuring MPLS TE, see [MPLS Traffic Engineering and Enhancements](#).

## Configuring the Tailend Routers

The tailend routers remove the MPLS labels from the IP multicast packets and send the packets to the MFIB for regular multicast forwarding processing. You must issue the **ip mroute** command to configure a static route back to the headend router, thus enabling RPF checks.

The following task explains how to configure PIM on the egress interface of the PE router. PIM is needed when the egress PE router is connected to a CE router, which is connected to a LAN where one or more multicast receivers are connected.

If the egress PE router is directly connected to a decoder device/system (e.g., DCM), you must configure Internet Group Management Protocol (IGMP) on the egress interface of the PE router. For more information on configuring IGMP, see [Customizing IGMP](#).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast mpls traffic-eng** [**range** *access-list-number* | *access-list-name*]
5. **interface** *type slot/port*  
or  
**interface** *type slot/port-adapter/port*
6. **ip pim** {**dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode**}
7. **exit**
8. **ip mroute** [**vrf** *vrf-name*] *source-address mask* {**fallback-lookup** {**global** | **vrf** *vrf-name*} | *rpf-address* | *interface-type interface-number*} [**distance**]
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>ip multicast-routing</b> [ <i>vrf vrf-name</i> ]<br>[ <i>distributed</i> ]<br><br><b>Example:</b><br>Router(config)# ip multicast-routing                                                                                                                        | Enables IP multicast routing globally.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 4 | <b>ip multicast mpls traffic-eng</b> [ <i>range</i><br><i>access-list-number</i>   <i>access-list-name</i> ]<br><br><b>Example:</b><br>Router(config)# ip multicast mpls traffic-eng                                                                                | Enables IP multicast routing for MPLS traffic engineering point-to-multipoint tunnels.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 5 | <b>interface type slot/port</b><br><br>or<br><br><b>interface type slot/port-adapter/port</b><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/1<br>or<br>Router(config)# interface fastethernet 1/0/0                                                | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>slot/</i> argument specifies the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port</i> argument specifies the port number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port-adapter/</i> argument specifies the port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.</li> </ul> |
| Step 6 | <b>ip pim</b> { <i>dense-mode</i> [ <i>proxy-register</i> { <i>list</i><br><i>access-list</i>   <i>route-map map-name</i> }]}   <b>passive</b>  <br><i>sparse-mode</i>   <i>sparse-dense-mode</i> }<br><br><b>Example:</b><br>Router(config-if)# ip pim ssm default | Enables Protocol Independent Multicast (PIM) on an interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                                                       | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|        | Command or Action                                                                                                                                                                                                                                             | Purpose                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| Step 8 | <pre>ip mroute [vrf vrf-name] source-address mask {fallback-lookup {global   vrf vrf-name}   rpf-address   interface-type interface-number} [distance]</pre> <p><b>Example:</b><br/>Router(config)# ip mroute 10.10.10.10<br/>255.255.255.255 10.11.11.11</p> | Configures a static multicast route (mroute) to the headend router, thus enabling RPF checks. |
| Step 9 | <pre>end</pre> <p><b>Example:</b><br/>Router(config)# end</p>                                                                                                                                                                                                 | (Required) Exits the current configuration mode and returns to privileged EXEC mode.          |

## Configuring Fast Reroute with P2MP TE Tunnels

To enable link protection for sub-LSPs associated with a P2MP TE tunnel, perform the following configuration tasks:

- Enable Fast Reroute on the headend router for each P2MP TE Tunnel.
- Configure P2P backup tunnels for network interfaces that require protection.

See [MPLS Traffic Engineering—Fast Reroute Link and Node Protection](#) for information and configuration instructions.

## Enabling MPLS Traffic Engineering System Logging of Events

MPLS Traffic Engineering system logging allows you to view the following events:

- Setting up and tearing down of LSPs
- RSVP Path and RESV requests
- Sub-LSP status (through path-change messages)

Commands to enable system logging include:

- `mpls traffic-eng logging lsp path-errors`
- `mpls traffic-eng logging lsp preemption`
- `mpls traffic-eng logging lsp reservation-errors`
- `mpls traffic-eng logging lsp setups`
- `mpls traffic-eng logging lsp teardowns`
- `mpls traffic-eng logging tunnel path change`

## Verifying the Configuration of MPLS Traffic Engineering Point-to-Multipoint Tunnels

This section includes the following tasks:

- [Verifying the Configuration of the Headend Router, page 20](#)

- [Verifying the Configuration of the Midpoint Routers, page 22](#)
- [Verifying the Configuration of the Tailend Routers, page 23](#)

## Verifying the Configuration of the Headend Router

At the headend router, use the following steps to verify that:

- All sub-LSPs are enabled.
- IP multicast traffic is being forwarded onto the P2MP TE tunnel.

The following commands may also be helpful in the verification of the headend router:

- **show cef path set** and **show cef path set detail** (when the headend router is also a branch point)
- **show ip mfib** and **show ip mfib verbose**
- **show ip rsvp fast-reroute**
- **show mpls traffic-eng destination list**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng tunnels** with the **dest-mode p2mp**, **detail**, and **summary** keywords

## SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels brief**
3. **show mpls traffic-eng forwarding path-set brief**
4. **show mpls traffic-eng forwarding path-set detail**
5. **show ip mroute**

## DETAILED STEPS

### Step 1 enable

Issue the **enable** command to enter privileged EXEC mode.

### Step 2 show mpls traffic-eng tunnels brief

Use the **show mpls traffic-eng tunnels brief** command to display the P2MP TE tunnels originating from the headend router. For example:

```
Router# show mpls traffic-eng tunnels brief
```

```
signaling Summary:
```

```
  LSP Tunnels Process:      running
  Passive LSP Listener:     running
  RSVP Process:             running
  Forwarding:               enabled
  Periodic reoptimization:  every 60 seconds, next in 5 seconds
  Periodic FRR Promotion:   Not Running
  Periodic auto-bw collection: disabled
```

```
P2P TUNNELS:
```

| TUNNEL NAME | DESTINATION | UP IF | DOWN IF | STATE/PROT |
|-------------|-------------|-------|---------|------------|
| p2p-LSP     | 10.2.0.1    | -     | Se2/0   | up/up      |

```
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
```



P2MP TUNNELS:

| INTERFACE | STATE/PROT | UP/CFG | DEST<br>TUNID | CURRENT<br>LSPID |
|-----------|------------|--------|---------------|------------------|
| Tunnel2   | up/up      | 3/10   | 2             | 1                |
| Tunnel5   | up/down    | 1/10   | 5             | 2                |

Displayed 2 (of 2) P2MP heads

P2MP SUB-LSPS:

| SOURCE          | TUNID | LSPID | DESTINATION     | SUBID | ST UP IF | DOWN IF |
|-----------------|-------|-------|-----------------|-------|----------|---------|
| 10.1.0.1        | 2     | 1     | 10.2.0.1        | 1     | up head  | Se2/0   |
| 10.1.0.1        | 2     | 1     | 10.3.0.199      | 2     | up head  | Et2/0   |
| 10.1.0.1        | 2     | 1     | 19.4.0.1        | 2     | up head  | s2/0    |
| 10.1.0.1        | 2     | 2     | 1 9.4.0.1       | 2     | up head  | s2/0    |
| 10.1.0.1        | 5     | 2     | 10.5.0.1        | 7     | up head  | e2/0    |
| 100.100.100.100 | 1     | 3     | 200.200.200.200 | 1     | up ge2/0 | s2/0    |
| 100.100.100.100 | 1     | 3     | 10.1.0.1        | 1     | up e2/0  | tail    |

Displayed 7 P2MP sub-LSPs:  
5 (of 5) heads, 1 (of 1) midpoints, 1 (of 1) tails

### Step 3 show mpls traffic-eng forwarding path-set brief

Use the **show mpls traffic-eng forwarding path-set brief** command to show the sub-LSPs that originate from the headend router. The following example shows three sub-LSPs originating at the headend router and going to different destinations. All the sub-LSPs belong to the same path set, which is a collection of paths. The path set is given a unique ID, which is shown in the PSID column of the example:

Router# **show mpls traffic-eng forwarding path-set brief**

| Sub-LSP Identifier<br>src_lspid[subid]->dst_tunid | InLabel | Next Hop | I/F   | PSID     |
|---------------------------------------------------|---------|----------|-------|----------|
| 10.0.0.1_19[16]->10.0.0.8_1                       | none    | 10.0.1.2 | Et0/0 | C5000002 |
| 10.0.0.1_19[27]->10.0.0.6_1                       | none    | 10.0.1.2 | Et0/0 | C5000002 |
| 10.0.0.1_19[31]->10.0.0.7_1                       | none    | 10.0.1.2 | Et0/0 | C5000002 |

### Step 4 show mpls traffic-eng forwarding path-set detail

Use the **show mpls traffic-eng forwarding path-set detail** command to show more information about the sub-LSPs that originate from the headend router. For example:

Router# **show mpls traffic-eng forwarding path-set detail**

```
LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
  Destination: 10.2.0.1, P2MP Subgroup ID: 1
    Path Set ID: 0x30000001
    OutLabel : Serial2/0, 16
    Next Hop : 10.1.3.2
    FRR OutLabel : Tunnel666, 16

LSP: Source: 10.1.0.1, TunID: 100, LSPID: 7
  Destination: 10.3.0.1, P2MP Subgroup ID: 2
    Path Set ID: 0x30000001
    OutLabel : Serial2/0, 16
    Next Hop : 10.1.3.2
    FRR OutLabel : Tunnel666, 16
```

### Step 5 show ip mroute

Use the **show ip mroute** command to verify that IP multicast traffic is being forwarded to the P2MP TE tunnel. In the following example, the output shown in bold shows that Tunnel 1 is part of the outgoing interface list for multicast group 232.0.1.4 with a source address of 10.10.10.10:

```

Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.10.10, 232.0.1.4), 1d00h/stopped, flags: sTI
  Incoming interface: Ethernet2/0, RPF nbr 10.10.1.1
  Outgoing interface list:
    Tunnel1, Forward/Sparse-Dense, 1d00h/00:01:17

(*, 224.0.1.40), 1d00h/00:02:48, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet2/0, Forward/Sparse, 1d00h/00:02:48

```

## Verifying the Configuration of the Midpoint Routers

At the midpoint router, use the following commands to verify that MPLS forwarding occurs. If the midpoint router is branch router, you can also use **show mpls forwarding-table labels** command to display show specific labels.

### SUMMARY STEP

1. **enable**
2. **show mpls forwarding-table**

### DETAILED STEP

#### Step 1 **enable**

Issue the **enable** command to enter privileged EXEC mode.

#### Step 2 **show mpls forwarding-table**

Use the **show mpls forwarding-table** command to show that MPLS packets are switched at the midpoint routers. For example:

```
Router# show mpls forwarding-table
```

| Local Label | Outgoing Label | Prefix or Tunnel Id | Bytes Switched | Label | Outgoing interface | Next Hop  |
|-------------|----------------|---------------------|----------------|-------|--------------------|-----------|
| 16          | 16             | 10.0.0.1 1 [19]     | 0              |       | Et1/0              | 10.0.1.30 |

```
Router# show mpls forwarding-table detail
```

| Local Label                                 | Outgoing Label | Prefix or Tunnel Id | Bytes Switched | Label | Outgoing interface | Next Hop  |
|---------------------------------------------|----------------|---------------------|----------------|-------|--------------------|-----------|
| 16                                          | 16             | 10.0.0.1 1 [19]     | 0              |       | Et1/0              | 10.0.1.30 |
| MAC/Encaps=14/18, MRU=1500, Label Stack{16} |                |                     |                |       |                    |           |
| AABBCC032800AABBCC0325018847 00010000       |                |                     |                |       |                    |           |

```
No output feature configured
Broadcast
```

## Verifying the Configuration of the Tailend Routers

At the tailend router, use the following steps to verify that:

- MPLS forwarding occurs.
- IP Multicast forwarding occurs.

You can also use the **show ip mfib**, **show mpls traffic-eng destination list**, and **show mpls traffic-eng tunnels dest-mode p2mp** commands for verification.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table**
3. **show ip mroute**

### DETAILED STEPS

#### Step 1 **enable**

Issue the **enable** command to enter privileged EXEC mode.

#### Step 2 **show mpls forwarding-table**

Use the **show mpls forwarding-table** command to show that MPLS labeled packets are forwarded from the tailend router without any label.

```
Router# show mpls forwarding-table
```

| Local Label | Outgoing Label | Prefix or Tunnel Id | Bytes Label Switched | Outgoing interface | Next Hop |
|-------------|----------------|---------------------|----------------------|--------------------|----------|
| 17          | [T] No Label   | 10.0.0.1 1 [19]     | 342                  | aggregate          |          |

```
[T] Forwarding through a LSP tunnel.
```

```
Router# show mpls forwarding-table detail
```

| Local Label | Outgoing Label | Prefix or Tunnel Id | Bytes Label Switched | Outgoing interface | Next Hop |
|-------------|----------------|---------------------|----------------------|--------------------|----------|
| 17          | No Label       | 10.0.0.1 1 [19]     | 342                  | aggregate          |          |

MAC/Encaps=0/0, MRU=0, Label Stack{}, via Ls0

#### Step 3 **show ip mroute**

Use the **show ip mroute** command to display IP multicast traffic. In the following example, the output in bold shows the incoming interface is Lspvif0 and the outgoing interface is Ethernet1/0 is for multicast group 232.0.1.4 with source address 10.10.10.10:

```
Router# show ip mroute
```

```
IP Multicast Routing Table
```

```
...
```

```
(*, 232.0.1.4), 1d02h/stopped, RP 0.0.0.0, flags: SP
Incoming interface: Null, RPF nbr 0.0.0.0
```

```
Outgoing interface list: Null

(10.10.10.10, 232.0.1.4), 00:01:51/00:01:38, flags:
  Incoming interface: Lspvif0, RPF nbr 10.0.0.1, Mroute
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse, 00:01:51/00:02:37

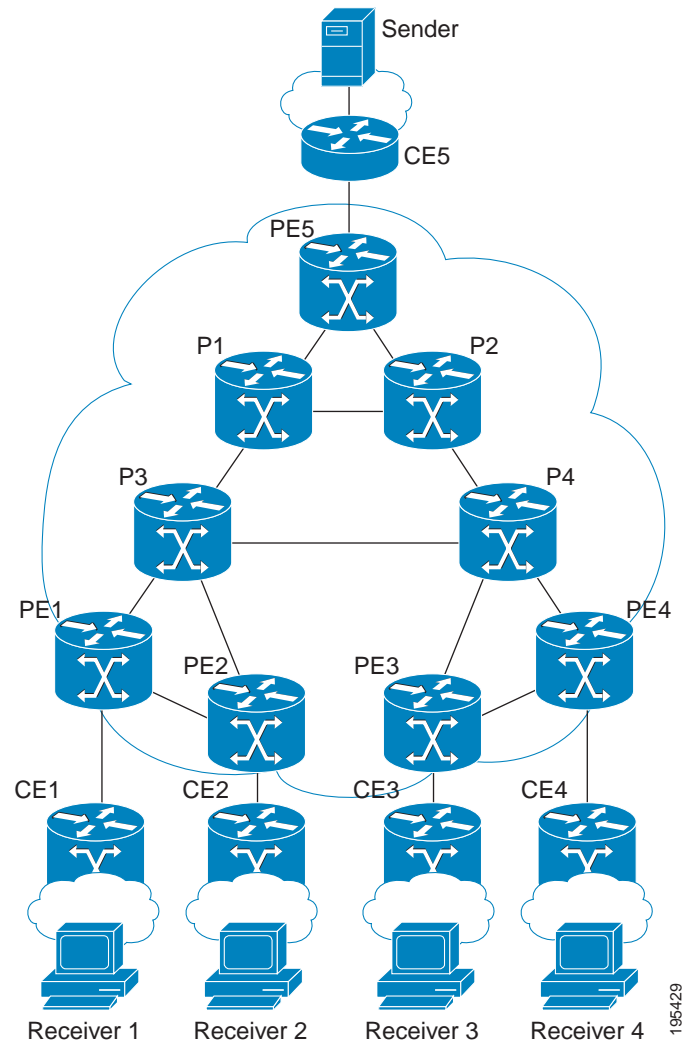
(*, 224.0.1.40), 1d02h/00:02:57, RP 0.0.0.0, flags: DCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Ethernet1/0, Forward/Sparse, 1d02h/00:02:57
```

## Configuration Examples for MPLS Point-to-Multipoint Traffic Engineering

The following examples show point-to-multipoint traffic engineering configurations on the headend router (PE5), a midpoint router (P1), and a tailend router (PE1):

- [Configuration of the Headend Router \(PE5\): Example, page 25](#)
- [Configuration of the Midpoint Router \(P1\): Example, page 28](#)
- [Configuration of the Tailend Router \(PE1\): Example, page 29](#)

**Figure 7**      **Sample MPLS TE P2MP TE Topology**



## Configuration of the Headend Router (PE5): Example

In the following example configuration of the headend router, note the following:

- IPv4 multicast routing is enabled with the **ip multicast-routing** command.
- Two destination lists are specified, one for dynamic paths and one for explicit paths. The destination list specifies one path-option per destination.
- The **tunnel mode mpls traffic-eng point-to-multipoint** command enables the P2MP tunnel.
- On the tunnel interfaces, the **ip pim passive** command is used.
- On the non-MPLS interfaces, the **ip pim sparse-mode** command is used.
- The **ip igmp static-group** commands map the multicast groups to the P2MP tunnel.
- Fast Reroute is enabled on the router, with tunnel 3 as the backup path. An explicit path called PE5->P1-BKUP provides the alternative path.

```

hostname [PE5]
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
ip source-route
ip cef
no ip domain lookup
!
ip multicast-routing
!
no ipv6 cef
mpls traffic-eng tunnels
!
mpls traffic-eng destination list name P2MP-DYN-DST-LIST
    ip 172.16.255.1 path-option 10 dynamic
    ip 172.16.255.2 path-option 10 dynamic
    ip 172.16.255.3 path-option 10 dynamic
    ip 172.16.255.4 path-option 10 dynamic
!
mpls traffic-eng destination list name P2MP-EXCIT-DST-LIST
    ip 172.16.255.1 path-option 10 explicit identifier 101
    ip 172.16.255.2 path-option 10 explicit identifier 102
    ip 172.16.255.3 path-option 10 explicit identifier 103
    ip 172.16.255.4 path-option 10 explicit identifier 104
!
multilink bundle-name authenticated
!
interface Tunnel1
    description PE5->PE1,PE2,PE3,PE4-DYN
    ip unnumbered Loopback0
    ip pim passive
    ip igmp static-group 232.0.1.4 source 192.168.5.255
    ip igmp static-group 232.0.1.3 source 192.168.5.255
    ip igmp static-group 232.0.1.2 source 192.168.5.255
    ip igmp static-group 232.0.1.1 source 192.168.5.255
    tunnel mode mpls traffic-eng point-to-multipoint
    tunnel destination list mpls traffic-eng name P2MP-DYN-DST-LIST
    tunnel mpls traffic-eng priority 7 7
    tunnel mpls traffic-eng bandwidth 10000
!
interface Tunnel2
    description PE5->PE1,PE2,PE3,PE4-EXCIT
    ip unnumbered Loopback0
    ip pim passive
    ip igmp static-group 232.0.1.8 source 192.168.5.255
    ip igmp static-group 232.0.1.7 source 192.168.5.255
    ip igmp static-group 232.0.1.6 source 192.168.5.255
    ip igmp static-group 232.0.1.5 source 192.168.5.255
    tunnel mode mpls traffic-eng point-to-multipoint
    tunnel destination list mpls traffic-eng name P2MP-EXCIT-DST-LIST
    tunnel mpls traffic-eng priority 7 7
    tunnel mpls traffic-eng bandwidth 20000
    tunnel mpls traffic-eng fast-reroute
!
interface Tunnel3
    description PE5->P1
    ip unnumbered Loopback0
    tunnel mode mpls traffic-eng
    tunnel destination 172.16.255.201

```

```
tunnel mpls traffic-eng path-option 10 explicit name PE5->P1-BKUP
!
interface Loopback0
 ip address 172.16.255.5 255.255.255.255
!
interface Ethernet0/0
 description CONNECTS to CE5
 ip address 192.168.5.1 255.255.255.252
 ip pim sparse-mode
!
interface Ethernet1/0
 description CONNECTS TO P1
 bandwidth 1000000
 ip address 172.16.0.13 255.255.255.254
 ip router isis
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel3
 isis network point-to-point
 ip rsvp bandwidth percent 100
!
interface Ethernet2/0
 description CONNECTS TO P2
 bandwidth 1000000
 ip address 172.16.0.14 255.255.255.254
 ip router isis
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth percent 100
!
router isis
 net 49.0001.1720.1625.5005.00
 is-type level-2-only
 metric-style wide
 passive-interface Loopback0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng level-2
!
!
ip classless
!
no ip http server
!
ip pim ssm default
!
ip explicit-path identifier 101 enable
 next-address 172.16.0.12
 next-address 172.16.192.0
 next-address 172.16.0.0
!
ip explicit-path identifier 102 enable
 next-address 172.16.0.12
 next-address 172.16.192.0
 next-address 172.16.0.3
!
ip explicit-path identifier 103 enable
 next-address 172.16.0.12
 next-address 172.16.192.0
 next-address 172.16.192.6
 next-address 172.16.0.6
!
ip explicit-path identifier 104 enable
 next-address 172.16.0.12
 next-address 172.16.192.0
 next-address 172.16.192.6
```

```

next-address 172.16.0.9
!
ip explicit-path name PE5->P1-BKUP enable
next-address 172.16.0.15
next-address 172.16.192.2

```

## Configuration of the Midpoint Router (P1): Example

In the following example configuration of the midpoint router, note the following:

- MPLS Traffic Engineering is enabled both globally and on the interface connecting to other core routers.
- MPLS TE extensions are enabled through the **mpls traffic-eng router-id** and **mpls traffic-eng level** commands.

```

hostname [P1]
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
ip source-route
ip cef
no ip domain lookup
!
no ipv6 cef
mpls traffic-eng tunnels
multilink bundle-name authenticated
!
interface Loopback0
 ip address 172.16.255.201 255.255.255.255
!
interface Ethernet0/0
 description CONNECTS TO P2
 bandwidth 1000000
 ip address 172.16.192.2 255.255.255.254
 ip router isis
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth percent 100
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 description CONNECTS TO P3
 bandwidth 1000000
 ip address 172.16.192.1 255.255.255.254
 ip router isis
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth percent 100
!

```



```

interface Ethernet2/0
  description CONNECTS TO PE5
  bandwidth 1000000
  ip address 172.16.0.12 255.255.255.254
  ip router isis
  mpls traffic-eng tunnels
  isis network point-to-point
  ip rsvp bandwidth percent 100
!
router isis
  net 49.0001.1720.1625.5201.00
  is-type level-2-only
  metric-style wide
  passive-interface Loopback0
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng level-2
!
ip classless
!
no ip http server

```

## Configuration of the Tailend Router (PE1): Example

In the following example configuration of the tailend router, note the following:

- IPv4 multicast routing is enabled with the **ip multicast-routing** command.
- On the non-MPLS interfaces, the **ip pim sparse-mode** command is used.
- The **ip multicast mpls** commands enable multicast routing of traffic.

```

hostname [PE1]
!
no aaa new-model
clock timezone PST -8
ip subnet-zero
ip source-route
ip cef
no ip domain lookup
!
ip multicast-routing
!
no ipv6 cef
mpls traffic-eng tunnels
multilink bundle-name authenticated
!
interface Loopback0
  ip address 172.16.255.1 255.255.255.255
!
interface Ethernet0/0
  description CONNECTS TO CE1
  ip address 192.168.1.1 255.255.255.252
  ip pim sparse-mode
!
interface Ethernet0/3
  description CONNECTS TO P3
  bandwidth 155000
  no ip address
  shutdown
  mpls traffic-eng tunnels
  ip rsvp bandwidth 155000
!
interface Ethernet1/0

```

```

description CONNECTS TO PE2
bandwidth 1000000
ip address 172.16.0.5 255.255.255.254
ip router isis
mpls traffic-eng tunnels
isis network point-to-point
ip rsvp bandwidth percent 100
!
interface Ethernet2/0
description CONNECTS TO P3
bandwidth 1000000
ip address 172.16.0.0 255.255.255.254
ip router isis
mpls traffic-eng tunnels
isis network point-to-point
ip rsvp bandwidth percent 100
!
router isis
net 49.0001.1720.1625.5001.00
is-type level-2-only
metric-style wide
passive-interface Loopback0
mpls traffic-eng router-id Loopback0
mpls traffic-eng level-2
!
!
ip classless
!
no ip http server

!
ip multicast mpls traffic-eng
ip pim ssm default
ip mroute 192.168.5.0 255.255.255.0 172.16.255.5

```

## Additional References

The following sections provide references related to the P2MP TE feature.

## Related Documents

| Related Topic                           | Document Title                                                                 |
|-----------------------------------------|--------------------------------------------------------------------------------|
| MPLS Traffic Engineering Fast Reroute   | <a href="#">MPLS Traffic Engineering—Fast Reroute Link and Node Protection</a> |
| MPLS Traffic Engineering LSP Attributes | <a href="#">MPLS Traffic Engineering—LSP Attributes</a>                        |

## Standards

| Standard                                | Title                                                                                                                             |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| draft-leroux-mpls-p2mp-te-bypass-xx.txt | <i>P2MP MPLS-TE Fast Reroute with P2MP Bypass Tunnels</i>                                                                         |
| draft-ietf-mpls-p2mp-te-mib-09.txt      | <i>Point-to-Multipoint Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB) module</i> |

## MIBs

| MIB                          | MIBs Link                                                                                                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                                        |
|----------|------------------------------------------------------------------------------|
| RFC 4875 | <i>Extensions to RSVP-TE for Point-to-Multipoint TE Label Switched Paths</i> |
| RFC 4461 | <i>Signaling Requirements for Point-to-Multipoint TE MPLS LSPs</i>           |
| RFC 5332 | <i>MPLS Multicast Encapsulations</i>                                         |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Glossary

**Branch router**—An router that has more than one directly connected downstream routers. A router where packet replication occurs.

**Bud router**— An egress router that has one or more directly connected downstream routers. A bud node can be a branch node and a destination.

**Crossover**—A condition that occurs at an intersecting node when two or more incoming sub-LSPs that belong to the same LSP have different input interfaces and different output interfaces.

**Egress router**— One of potentially many destinations of the P2MP TE sub-LSP. Egress routers may also be referred to as tailend routers, leaf nodes, or leaves.

**Data Duplication**—A condition that occurs when an egress router receives duplicate packets. The condition can happen as a result of re-optimization of LSPs, remerge, or crossover. It causes network bandwidth to be wasted and should be minimized.

**Grafting**— The process of adding a new sub-LSP to a P2MP TE tunnel.

**Headend router**— An Ingress PE router that is at the “headend” of a P2MP tunnel.

**Ingress router**— The router that initiates the signaling messages that set up the P2MP TE LSP. Also known as the headend router.

**MDT**— A Multicast Domain/Distribution tree in the core which carries traffic and/or control messages for a given VPN. An MDT implicitly implies that we are discussing the Domain-Model. And MDT can have multiple types of encapsulation in the core, e.g. GRE, IP-in-IP or MPLS.

**MFI**— MPLS Forwarding Infrastructure

**P2MP ID (P2ID)**— A unique identifier of a P2MP TE LSP, which is constant for the whole LSP regardless of the number of branches and/or leaves.

**P2MP LSP**—one or more source to leaf sub-LSPs. It is identified by 5-tuple key:

Session

- P2MP ID
- Tunnel ID
- Extended Tunnel ID

Sender Template

- Tunnel sender address
- LSP ID

**P2MP Sub-LSP**—A segment of a P2MP TE LSP that runs from the headend router to one destination. A sub-LSP is identified by the following 7-tuple key:

P2MP session

- P2MP ID
- Tunnel ID
- Extended Tunnel ID

Sender Template

- Tunnel sender address
- LSP ID
- Sub Group ID originator
- Sub Group ID

**P2MP-TE**—Point to Multipoint Traffic Engineering

**P2MP tree**— The ordered set of routers and TE links that comprise the paths of P2MP TE sub-LSPs from the ingress router to all of the egress routers.

**P2MP tunnel**—A group of one or more P2MP LSPs. A tunnel has the following 3-tuple key:

- P2MP ID
- Tunnel ID
- Extended Tunnel ID.

**PIM**—Protocol Independent Multicast

**PIM-SM**—PIM Sparse Mode, see RFC 4601

**PIM-SSM**—PIM Source Specific Multicast, a subset of PIM-SM. See RFC 4601.

**Pruning**—The process of removing a sub-LSP from a P2MP LSP.

**Receiver**— A recipient of traffic carried on a P2MP service supported by a P2MP sub-LSP. A receiver is not necessarily an egress router of the P2MP LSP. Zero, one, or more receivers may receive data through a given egress router.

**Remerge**—A condition that occurs at an intersecting node when two data streams belonging to the same P2MP LSP merge into onto one data stream as they exit the intersecting node.

**Sibling LSP**—Two LSPs that belong to the same P2MP tunnel, meaning that the session objects are the same for both LSPs.

**Sibling sub-LSP**—Two sub-LSPs that belong to the same P2MP LSP, meaning that the session and sender template objects are the same for both sub-LSPs.

**Source**—The sender of traffic that is carried on a P2MP service supported by a P2MP LSP. The sender is not necessarily the ingress router of the P2MP LSP.

**Tailend router**— An Egress PE router that is at the “tailend” of a P2MP tunnel.

# Feature Information for MPLS Point-to-Multipoint Traffic Engineering

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Point-to-Multipoint Traffic Engineering

| Feature Name                                 | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Point-to-Multipoint Traffic Engineering | 12.2(33)SRE | <p>The MPLS Point-to-Multipoint Traffic Engineering feature enables you to forward MPLS traffic from one source to multiple destinations.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was introduced.</p> <p>The following commands were introduced or modified:</p> <pre> debug ip rsvp p2mp, debug mpls traffic-eng filter debug mpls traffic-eng path ip multicast mpls traffic-eng ip path-option ip pim show cef show ip multicast mpls vif show ip rsvp fast-reroute show ip rsvp fast-reroute bw-protect show ip rsvp fast-reroute detail show ip rsvp request show ip rsvp reservation show ip rsvp sender show mpls traffic-eng destination list show mpls traffic-eng fast-reroute database show mpls traffic-eng forwarding path-set show mpls traffic-eng forwarding statistics show mpls traffic-eng tunnels tunnel destination list mpls traffic-eng tunnel mode mpls traffic-eng point-to-multipoint </pre> |

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

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

© 2009 Cisco Systems, Inc. All rights reserved.







## **MPLS Traffic Engineering: DiffServ**





## MPLS Traffic Engineering - DiffServ Aware (DS-TE)

---

This guide presents extensions made to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it DiffServ aware. Specifically, the bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through at least two bandwidth pools: a *global pool* (also called BC0) and a *sub-pool* (also called BC1). The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.

Beginning with Cisco IOS Release 12.2(33)SRB, DS-TE has been augmented to conform to IETF standards that were developed after the initial creation of Cisco DS-TE. Now both the traditional and the IETF versions of DS-TE can be run on your network; the new releases are backwards compatible.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

## Feature History

| Release       | Modification                                                                                                                                                                                 |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12.0(11) ST   | DS-TE feature introduced.                                                                                                                                                                    |
| 12.0(14) ST   | Support was added for Cisco Series 7500(VIP) platform.<br>Support was added for IS-IS Interior Gateway Protocol.                                                                             |
| 12.0(14) ST-1 | Support was added for guaranteed bandwidth service directed to many destination prefixes (for example, guaranteed bandwidth service destined to an autonomous system or to a BGP community). |
| 12.0(22)S     | Feature was implemented in Cisco IOS Release 12.0(22)S.                                                                                                                                      |
| 12.2(14)S     | Feature was integrated into Cisco IOS Release 12.2(14)S.                                                                                                                                     |
| 12.2(18)S     | Feature was implemented in Cisco IOS Release 12.2(18)S.                                                                                                                                      |
| 12.2(18)SXD   | Feature was implemented in Cisco IOS Release 12.2(18)SXD.                                                                                                                                    |
| 12.2(28)SB    | Feature was implemented in Cisco IOS Release 12.2(28)SB.                                                                                                                                     |
| 12.2(33)SRB   | Feature was augmented to include the new IETF-Standard functionality of DS-TE, as described in RFCs 3270, 4124, 4125, and 4127.                                                              |

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

The guide contains the following sections:

- [Background and Overview, page 2](#)
- [Supported Standards, page 5](#)
- [Prerequisites, page 6](#)
- [Configuration Tasks, page 6](#)
- [Configuration Examples, page 13](#)
- [Command Reference, page 40](#)
- [Glossary, page 41](#)

## Background and Overview

MPLS traffic engineering allows constraint-based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. DiffServ-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of “guaranteed” traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool. In the new IETF-Standard, the global pool is called BC0 and the sub-pool is called BC1. These are two of an

eventually available eight Class Types). This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance in terms of delay, jitter, or loss for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming that QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate “overbooking” ratios for guaranteed and regular traffic. In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements such as real-time voice, virtual IP leased line, and bandwidth trading, where over-engineering cannot be assumed everywhere in the network.

The new IETF-Standard functionality of DS-TE expands the means for allocating constrained bandwidth into two distinct models, called the “Russian Dolls Model” and the “Maximum Allocation Model”. They differ from each other as follows:

**Table 1** *Bandwidth Constraint Model Capabilities*

| MODEL                     | Achieves Bandwidth Efficiency | Ensures Isolation across Class Types |                         | Protects against QoS Degradation... |                             |
|---------------------------|-------------------------------|--------------------------------------|-------------------------|-------------------------------------|-----------------------------|
|                           |                               | When Preemption is Not Used          | When Preemption is Used | ...of the Premium Class Type        | ...of all other Class Types |
| <b>Maximum Allocation</b> | Yes                           | Yes                                  | Yes                     | Yes                                 | No                          |
| <b>Russian Dolls</b>      | Yes                           | No                                   | Yes                     | Yes                                 | Yes                         |

Therefore in practice, a Network Administrator might prefer to use:

- the Maximum Allocation Model when s/he needs to ensure isolation across all Class Types without having to use pre-emption, and s/he can afford to risk some QoS degradation of Class Types other than the Premium Class.
- the Russian Dolls Model when s/he needs to prevent QoS degradation of all Class Types and can impose pre-emption.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool or class-type bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

With the addition of IETF-Standard functionality (beginning with Cisco IOS Release 12.2(33)SRB), networks may accomplish DS-TE in three different combinations or “modes”, so that they may transition to the IETF-Standard formats in a manner that will not degrade their ongoing traffic service. These three situations or modes are summarized as follows:

1. **The original, or “Traditional” (pre-IETF-Standard) mode.** This describes networks that already operate the form of DS-TE that was introduced by Cisco a few years ago. Such networks can continue to operate in this traditional mode, even when they use the new Release 12.2(33)SRB and subsequent releases.
2. **The “Migration” or combination mode.** Networks already running traditional DS-TE that would like to upgrade to the IETF-Standard should first configure their routers into the Migration mode. This will allow them to continue to operate DS-TE without tunnels being torn down. In Migration mode, routers will continue to generate IGP and tunnel signalling as in the Traditional form, but now these routers will add TE-class mapping and will accept advertisement in both the Traditional and the new IETF-Standard formats.
3. **The “Liberal IETF” mode.** Networks already running in the Migration mode can then move into IETF formats by reconfiguring their routers into this flexible (hence “Liberal”) combination: their routers will henceforth generate IGP advertisement and tunnel signalling according to the new IETF Standard, but they will remain capable of accepting advertisement in the Traditional format, as well as in the new IETF format.

Table 2 summarizes these distinctions among the three modes.

**Table 2** *Summary of DS-TE Mode behaviors*

| MODE                | Uses<br>TE-class<br>mapping | Generates            |                       | Processes                |                       |
|---------------------|-----------------------------|----------------------|-----------------------|--------------------------|-----------------------|
|                     |                             | IGP<br>Advertisement | RSVP-TE<br>Signalling | IGP<br>Advertisement     | RSVP-TE<br>Signalling |
| <b>Traditional</b>  | No                          | traditional          | traditional           | traditional <sup>1</sup> | traditional           |
| <b>Migration</b>    | Yes                         | traditional          | traditional           | traditional &<br>IETF    | traditional &<br>IETF |
| <b>Liberal IETF</b> | Yes                         | IETF                 | traditional &<br>IETF | traditional &<br>IETF    | traditional &<br>IETF |

<sup>1</sup>Note that it is not possible for the Traditional mode to be liberal in what it accepts in terms of IGP, since it does not use TE-Class mapping and therefore cannot interpret the “Unreserved Bandwidth” in the IETF-compliant way when the Subpool Sub-TLV is absent.

## Benefits

DiffServ-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on *signaled* rather than *provisioned* QoS
- Build the higher-revenue generating “strict-commitment” QoS services, without over-provisioning

- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS.

## Related Features and Technologies

The DS-TE feature is related to OSPF, IS-IS, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

## Related Documents

The following sections provide references related to the MPLS Traffic Engineering—DiffServ Aware (DS-TE) feature:

| Related Topic            | Document Title                                                                                                                                                                      |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IS-IS                    | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li> <li>• <a href="#">Configuring a Basic IS-IS Network</a></li> </ul>   |
| MPLS Traffic Engineering | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                                                                           |
| OSPF                     | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li> <li>• <a href="#">OSPF Configuration Task List</a></li> </ul>        |
| QoS                      | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a></li> <li>• <a href="#">Quality of Service Overview</a></li> </ul> |
| RSVP                     | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a></li> <li>• <a href="#">Configuring RSVP</a></li> </ul>            |

## Supported Standards

The traditional (pre-IETF Standard) version of DiffServ-aware MPLS Traffic Engineering conforms to the descriptions given in the following two documents:

- *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham
- *Protocol Extensions for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, J. Boyle, K. Kompella, W. Townsend & D. Skalecki.

The IETF Standard for DiffServ-aware MPLS Traffic Engineering is described in the following four documents:

- [Multi-Protocol Label Switching \(MPLS\) Support of Differentiated Services](#) by F. Le Faucheur, L. Wu, B. Davie, P. Vaananen, R. Krishnan, P. Cheval, & J. Heinanen (RFC 3270)
- [Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering](#) ed. by F. Le Faucheur (RFC 4124)
- [Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering](#) ed. by F. Le Faucheur (RFC 4127)

- [\*Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering\*](#) by F. Le Faucheur & W. Lai (RFC 4125).

The new concept of "Class-Type" defined in the IETF Standard corresponds to the prior concept of "bandwidth pool" that was implemented in the original version of DS-TE. Likewise, the two bandwidth pools implemented in the original version of DS-TE (global pool and sub-pool) correspond to two of the IETF Standard's new Class-Types (Class-Type 0 and Class-Type 1, respectively).

## Prerequisites

Your network must support the following Cisco IOS features in order to support guaranteed bandwidth services based on DiffServ-aware Traffic Engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- OSPF or ISIS
- RSVP-TE
- QoS

## Configuration Tasks

This section presents the minimum set of commands you need to implement the DiffServ-aware Traffic Engineering feature—in other words, to establish a tunnel that reserves bandwidth to a sub-pool (renamed BC1 by the IETF-Standard).

The subsequent "[Configuration Examples](#)" section ([page 13](#)), presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

## From Traditional to IETF-Standard Commands

DS-TE commands originally were developed from the then-existing command set that had been used to configure MPLS traffic engineering. The only difference introduced at that time to create DS-TE was the expansion of two commands:

- **ip rsvp bandwidth** was expanded to configure the size of the sub-pool on every link.
- **tunnel mpls traffic-eng bandwidth** was expanded to enable a TE tunnel to reserve bandwidth from the sub-pool.

### The ip rsvp bandwidth command

The early MPLS command had been

```
ip rsvp bandwidth x y
```

where x = the size of the only possible pool, and y = the size of a single traffic flow (ignored by traffic engineering).

Then, to create the original implementation of DS-TE, the command was made into

```
ip rsvp bandwidth x y sub-pool z
```

where x = the size of the global pool, and z = the size of the sub-pool.



With the addition of the IETF-Standard version of DS-TE, the command has been further extended to become:

```
ip rsvp bandwidth x y [ [rdm x {subpool z | bc1 z}] | [mam bc0 x bc1 z]]
```

where **x** = the size of the global pool (now called **bc0**), and **z** = the size of the sub-pool (now called also **bc1**).

Two bandwidth constraint models also have become available, “Russian Dolls” (indicated by the keyword **rdm**) and “Maximum Allocation” (**mam**). The former model allows greater sharing of bandwidth across all Class Types (bandwidth pools), while the latter protects especially the premium Class Type. (The IETF Standard makes possible the future implementation of as many as seven sub-pools within one LSP, instead of just one sub-pool per LSP).

## The tunnel mpls traffic-eng bandwidth command

The pre-DS-TE traffic engineering command was

```
tunnel mpls traffic-eng bandwidth b
```

where **b** = the amount of bandwidth this tunnel requires.

So for the original DS-TE, you specified from which pool (global or sub) the tunnel's bandwidth would come. You could enter

```
tunnel mpls traffic-eng bandwidth sub-pool b
```

to indicate that the tunnel should use bandwidth from the sub-pool. Alternatively, you could enter

```
tunnel mpls traffic-eng bandwidth b
```

to indicate that the tunnel should use bandwidth from the global pool (which was the default).

With the addition of the IETF-Standard version of DS-TE, the command has been extended to become:

```
tunnel mpls traffic-eng bandwidth [sub-pool|class-type 1] b
```

where both **sub-pool** and **class-type 1** indicate the same, smaller bandwidth pool (now called class-type 1). The two keywords can be used interchangeably.

## The mpls traffic-eng ds-te commands

The IETF Standard introduces two new commands, one to indicate the Bandwidth Constraints model

```
mpls traffic-eng ds-te bc-model [rdm | mam]
```

and one to select the DS-TE mode:

```
mpls traffic-eng ds-te mode [migration|ietf]
```

(The concepts of bc-model and DS-TE mode were explained on [page 3](#)).

The first command allows you to select between the Russian Dolls Model (**rdm**) and the Maximum Allocation Model (**mam**) of bandwidth constraints.

The second command allows you to transition a network from traditional DS-TE tunnels to the IETF Standard without disrupting any of the tunnels' operation. To accomplish this, you first put the routers into Migration mode (using the **migration** keyword) and subsequently into the Liberal-IETF mode (using the **ietf** keyword).

## Transitioning a Network to the IETF Standard

Networks already operating DS-TE tunnels by means of the traditional, pre-IETF-Standard software can switch to the IETF-Standard without interrupting their DS-TE service by following this sequence:

1. Install Cisco IOS Release 12.2(33)SRB (or a subsequent release) on each router in the network, gradually, one router at a time, using Cisco's In Service Software Upgrade (ISSU) procedure which protects ongoing network traffic from interruption. (After that installation, DS-TE tunnels in the network will continue to operate by using the pre-IETF-Standard formats.)
2. Enter the global configuration command **mpls traffic-eng ds-te mode migration** on each router in the network, one router at a time. This will enable the routers to receive IETF-format IGP advertisement and RSVP-TE signaling, while the routers will continue to generate and receive the pre-Standard formats for those two functions.
3. After all the routers in the network have begun to operate in Migration mode, enter the global configuration command **mpls traffic-eng ds-te mode ietf** on each router, one at a time. This will cause the router to refresh its TE tunnels with IETF-compliant Path signaling, without disrupting the tunnels' operation. This mode also causes the router to generate IGP advertisement in the IETF-Standard format.

## Configuring DS-TE Tunnels

To establish a sub-pool (BC1) traffic engineering tunnel, you must enter configurations at three levels:

- the device level (router or switch router)
- the physical interface
- the tunnel interface

On the first two levels, you activate traffic engineering; on the third level—the tunnel interface—you establish the sub-pool tunnel. Therefore, it is only at the tunnel headend device that you need to configure all three levels. At the tunnel midpoints and tail, it is sufficient to configure the first two levels.

In the tables below, each command is explained in brief. For a more complete explanation of any command, type it into the Command Lookup Tool at <http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl>. (If prompted to log in there, use your Cisco.com account username and password).

### Level 1: Configuring the Device

At this level, you tell the device (router or switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding or CEF), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, a bandwidth constraints model, and either the OSPF or IS-IS routing algorithm (Open Shortest Path First or Intermediate System to Intermediate System). This level is called the global configuration mode, because the configuration is applied globally, to the entire device, rather than to a specific interface or routing instance.

You enter the following commands:

|                | Command                                                                              | Purpose                                                                                                                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b>  | Router(config)# <b>ip cef distributed</b>                                            | Enables CEF—which accelerates the flow of packets through the device.                                                                                                                                                                   |
| <b>Step 2</b>  | Router(config)# <b>mpls traffic-eng tunnels</b>                                      | Enables MPLS, and specifically its traffic engineering tunnel capability.                                                                                                                                                               |
| <b>Step 3</b>  | Router(config)# <b>mpls traffic-eng ds-te bc-model [rdm   mam ]</b>                  | Specifies the bandwidth constraints model (see <a href="#">page 3</a> ).                                                                                                                                                                |
| <b>Step 4</b>  | Router(config)# <b>router ospf</b><br><br>[or]<br>Router(config)# <b>router isis</b> | Invokes the OSPF routing process for IP and puts the device into router configuration mode. Proceed now to Steps 10 and 11.<br><br>Alternatively, you may invoke the IS-IS routing process with this command, and continue with Step 5. |
| <b>Step 5</b>  | Router (config-router)# <b>net network-entity-title</b>                              | Specifies the IS-IS network entity title (NET) for the routing process.                                                                                                                                                                 |
| <b>Step 6</b>  | Router (config-router)# <b>metric-style wide</b>                                     | Enables the router to generate and accept IS-IS new-style TLVs (type, length, and value objects).                                                                                                                                       |
| <b>Step 7</b>  | Router (config-router)# <b>is-type level-n</b>                                       | Configures the router to learn about destinations inside its own area or “IS-IS level”.                                                                                                                                                 |
| <b>Step 8</b>  | Router (config-router)# <b>mpls traffic-eng level-n</b>                              | Specifies the IS-IS level (which must be same level as in the preceding step) to which the router will flood MPLS traffic-engineering link information.                                                                                 |
| <b>Step 9</b>  | Router (config-router)# <b>passive-interface loopback0</b>                           | Instructs IS-IS to advertise the IP address of the loopback interface without actually running IS-IS on that interface. Continue with Step 10 but don’t do Step 11—because Step 11 refers to OSPF.                                      |
| <b>Step 10</b> | Router(config-router)# <b>mpls traffic-eng router-id loopback0</b>                   | Specifies that the traffic engineering router identifier is the IP address associated with the <i>loopback0</i> interface.                                                                                                              |
| <b>Step 11</b> | Router(config-router)# <b>mpls traffic-eng area num</b>                              | Turns on MPLS traffic engineering for a particular OSPF area.                                                                                                                                                                           |

## Level 2: Configuring the Physical Interface

Having configured the device, you now must configure the interface on that device through which the tunnel will run. To do that, you first put the router into interface-configuration mode.

You then enable Resource Reservation Protocol (RSVP). This protocol is used to signal (set up) a traffic engineering tunnel, and to tell devices along the tunnel path to reserve a specific amount of bandwidth for the traffic that will flow through that tunnel. It is with this command that you establish the maximum size of the sub-pool (BC1).

Finally, you enable the MPLS traffic engineering tunnel feature on this physical interface—and if you will be relying on the IS-IS routing protocol, you enable that as well.

To accomplish these tasks, you enter the following commands:

|        | Command                                                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <i>interface-id</i>                                                                                                                                                                                                                          | Moves configuration to the interface level, directing subsequent configuration commands to the specific interface identified by the <i>interface-id</i> .                                                                                                                                            |
| Step 2 | Router(config-if)# <b>ip rsvp bandwidth</b> [ <i>interface-kbps</i> ] [ <i>single-flow-kbps</i> ][ <b>rdm</b> <i>kbps</i> { <b>subpool</b> <i>kbps</i> }[ <b>bc1</b> <i>subpool</i> ]}][ <b>max-reservable-bw</b> <i>kbps</i> <b>bc0</b> <i>kbps</i> <b>bc1</b> <i>kbps</i> ] | Enables RSVP on this interface, indicates the Bandwidth Constraints Model to be used (explained on <a href="#">page 3</a> ), and limits the amount of bandwidth RSVP can reserve on this interface. The sum of bandwidth used by all tunnels on this interface cannot exceed <i>interface-kbps</i> . |
| Step 3 | Router(config-if)# <b>mpls traffic-eng tunnels</b>                                                                                                                                                                                                                            | Enables the MPLS traffic engineering tunnel feature on this interface.                                                                                                                                                                                                                               |
| Step 4 | Router(config-if)# <b>ip router isis</b>                                                                                                                                                                                                                                      | Enables the IS-IS routing protocol on this interface. Do not enter this command if you are configuring for OSPF.                                                                                                                                                                                     |

### Level 3: Configuring the Tunnel Interface

Now you create a set of attributes for the tunnel itself; those attributes are configured on the “tunnel interface” (not to be confused with the physical interface just configured above).

You enter the following commands:

|        | Command                                                                                                               | Purpose                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b> <b>tunnel1</b>                                                                       | Creates a tunnel interface (named in this example <b>tunnel1</b> ) and enters interface configuration mode.                                                                                                     |
| Step 2 | Router(config-if)# <b>tunnel destination</b> <i>A.B.C.D</i>                                                           | Specifies the IP address of the tunnel tail device.                                                                                                                                                             |
| Step 3 | Router(config-if)# <b>tunnel mode mpls traffic-eng</b>                                                                | Sets the tunnel’s encapsulation mode to MPLS traffic engineering.                                                                                                                                               |
| Step 4 | Router(config-if)# <b>tunnel mpls traffic-eng bandwidth</b> { <i>sub-pool</i>   <i>class-type1</i> } <i>bandwidth</i> | Configures the tunnel’s bandwidth, and assigns it either to the sub-pool (when you use that keyword or the IETF-Standard keyword <b>class-type1</b> ) or to the global pool (when you leave out both keywords). |
| Step 5 | Router(config-if)# <b>tunnel mpls traffic-eng priority</b>                                                            | Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted.                                                                                                    |
| Step 6 | Router(config-if)# <b>tunnel mpls traffic-eng path-option</b>                                                         | Configures the paths (hops) a tunnel should use. The user can enter an explicit path (can specify the IP addresses of the hops) or can specify a dynamic path (the router figures out the best set of hops).    |

### Verifying the Configuration

To view the complete configuration you have entered, use the EXEC command **show running-config** and check its output display for correctness.

To check *just one tunnel’s* configuration, enter **show interfaces tunnel** followed by the tunnel interface number. And to see that tunnel’s RSVP bandwidth and flow, enter **show ip rsvp interface** followed by the name or number of the physical interface.

Here is an example of the information displayed by these latter two commands. (To see an explanation of each field used in the following displays, enter **show interfaces tunnel** or **show ip rsvp interface** into the Command Lookup Tool at <http://www.cisco.com/cgi-bin/Support/Cmdlookup/home.pl>. If prompted to log in there, use your Cisco.com account username and password.)

```
Router#show interfaces tunnel 4
Tunnel4 is up, line protocol is down
  Hardware is Routing Tunnel
  MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
  Tunnel source 0.0.0.0, destination 0.0.0.0
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets, 0 restarts

Router#show ip rsvp interface pos4/0
interface    allocated  i/f max  flow max  sub max
PO4/0        300K        466500K  466500K   0M
```

To view *all tunnels at once* on the router you have configured, enter **show mpls traffic-eng tunnels brief**. The information displayed when tunnels are functioning properly looks like this:

```
Router#show mpls traffic-eng tunnels brief
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:             running
  Forwarding:               enabled
  Periodic reoptimization:  every 3600 seconds, next in 3029 seconds
TUNNEL NAME DESTINATION    UP IF    DOWN IF    STATE/PROT
GSR1_t0 192.168.1.13      -        SR3/0      up/up
GSR1_t1 192.168.1.13      -        SR3/0      up/up
GSR1_t2 192.168.1.13      -        PO4/0      up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

When one or more tunnels is not functioning properly, the display could instead look like this. (In the following example, tunnels t0 and t1 are down, as indicated in the far right column).

```
Router#show mpls traffic-eng tunnels brief
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:             running
  Forwarding:               enabled
  Periodic reoptimization:  every 3600 seconds, next in 2279 seconds
TUNNEL NAME DESTINATION    UP IF    DOWN IF    STATE/PROT
GSR1_t0 192.168.1.13      -        SR3/0      up/down
GSR1_t1 192.168.1.13      -        SR3/0      up/down
GSR1_t2 192.168.1.13      -        PO4/0      up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

To find out *why* a tunnel is down, insert its name into this same command, after adding the keyword **name** and omitting the keyword **brief**. For example:

```
Router#show mpls traffic-eng tunnels name GSR1_t0
Name:GSR1_t0                               (Tunnel0) Destination:192.168.1.13
```

```
Status:
Admin:up          Oper:down Path: not valid      Signalling:connected
```

If, as in this example, the Path is displayed as **not valid**, use the **show mpls traffic-eng topology** command to make sure the router has received the needed updates.

Additionally, you can use any of the following **show** commands to inspect particular aspects of the network, router, or interface concerned:

| To see information about... |                                                          |                                                                                           |
|-----------------------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------|
| this level                  | and this item...                                         | Use this command                                                                          |
| Network                     | Advertised bandwidth allocation information              | <b>show mpls traffic-eng link-management advertisements</b>                               |
|                             | Preemptions along the tunnel path                        | <b>debug mpls traffic-eng link-management preemption</b>                                  |
|                             | Available TE link bandwidth on all head routers          | <b>show mpls traffic-eng topology</b> (described on <a href="#">page 41</a> )             |
| Router                      | Status of all tunnels currently signalled by this router | <b>show mpls traffic-eng link-management admission-control</b>                            |
|                             | Tunnels configured on midpoint routers                   | <b>show mpls traffic-eng link-management summary</b>                                      |
| Physical interface          | Detailed information on current bandwidth pools          | <b>show mpls traffic-eng link-management bandwidth-allocation</b> <i>[interface-name]</i> |
|                             | TE RSVP bookkeeping                                      | <b>show mpls traffic-eng link-management interfaces</b>                                   |
|                             | Entire configuration of one interface                    | <b>show run interface</b>                                                                 |

# Configuration Examples



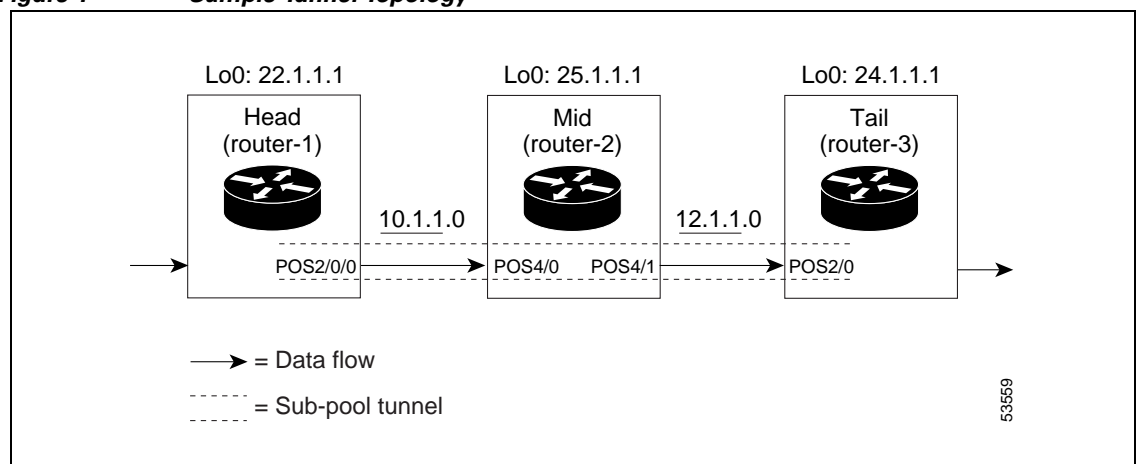
## Note

The following 25 pages of examples illustrate DS-TE in the traditional, pre-IETF-Standard mode. You may update these examples simply by inserting the new Device Level command **mpls traffic-eng ds-te bc-model** as its proper use is shown in Step 3 on [page 9](#), and by applying the updated syntax within the two modified commands as each is shown respectively at the Physical Interface Level in Step 2 on [page 10](#) (**ip rsvp bandwidth**), and at the Tunnel Interface Level in Step 4 on [page 10](#) (**tunnel mpls traffic-eng bandwidth**).

First this section presents the DS-TE configurations needed to create the sub-pool tunnel. Then it presents the more comprehensive design for building end-to-end guaranteed bandwidth service, which involves configuring Quality of Service as well.

As shown in [Figure 1](#), the tunnel configuration involves at least three devices—tunnel head, midpoint, and tail. On each of those devices one or two network interfaces must be configured, for traffic ingress and egress.

**Figure 1**      **Sample Tunnel Topology**



## Tunnel Head

At the device level:

```
router-1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis
    router-1(config-router)# net
    49.0000.1000.0000.0010.00
    router-1(config-router)# metric-style wide
    router-1(config-router)# is-type level-1
    router-1(config-router)#

router-1(config)# router ospf 100
    router-1(config-router)# redistribute connected
    router-1(config-router)# network 10.1.1.0 0.0.0.255 area 0
    router-1(config-router)# network 22.1.1.1 0.0.0.0 area 0
```

```

router-1(config-router)# mpls traffic-eng
level-1
router-1(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit

router-1(config)# interface Loopback0

```

At the virtual interface level:

```

router-1(config-if)# ip address 22.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS2/0/0

```

At the physical interface level (egress):

```

router-1(config-if)# ip address 10.1.1.1 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface Tunnel1

```

At the tunnel interface level:

```

router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 24.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-1(config-if)# exit
router-1(config)#

```

## Midpoint Devices

At the device level:

```

router-2# configure terminal
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels

```



[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> router-2(config)# <b>router isis</b> router-2(config-router)# <b>net</b> 49.0000.1000.0000.0012.00 router-2(config-router)# <b>metric-style wide</b> router-2(config-router)# <b>is-type level-1</b> router-2(config-router)# <b>mpls traffic-eng</b> <b>level-1</b> router-2(config-router)# <b>passive-interface</b> <b>Loopback0</b> [now one resumes the common command set]: router-2(config-router)# <b>mpls traffic-eng router-id Loopback0</b> router-2(config-router)# <b>exit</b> </pre> | <pre> router ospf 100 redistribute connected network 11.1.1.0 0.0.0.255 area 0 network 12.1.1.0 0.0.0.255 area 0 network 25.1.1.1 0.0.0.0 area 0 mpls traffic-eng area 0 </pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

```

router-2(config)# interface Loopback0

```

At the virtual interface level:

```

router-2(config-if)# ip address 25.1.1.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS4/0
router-1(config-if)# ip address 11.1.1.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000

```

[If using IS-IS instead of OSPF]:

```

router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS4/1
router-1(config-if)# ip address 12.1.1.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000

```

[If using IS-IS instead of OSPF]:

```

router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

Note that there is no configuring of tunnel interfaces at the mid-point devices, only network interfaces and the device globally.

## Tail-End Device

At the device level:

```

router-3# configure terminal
router-3(config)# ip cef distributed

```

```
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                               |                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-3(config)# router isis   router-3(config-router)# net     49.0000.1000.0000.0013.00   router-3(config-router)# metric-style wide   router-3(config-router)# is-type level-1    router-3(config-router)# mpls traffic-eng level-1   router-3(config-router)# passive-interface     Loopback0</pre> | <pre>router ospf 100   redistribute connected   network 12.1.1.0 0.0.0.255 area 0     network 24.1.1.1 0.0.0.0 area       0   mpls traffic-eng area 0</pre> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

```
router-3(config)# interface Loopback0
```

At the virtual interface level:

```
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# no ip directed-broadcast
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the device level:

```
router-1(config)# interface POS4/0
  router-1(config-if)# ip address 12.1.1.3 255.255.255.0
  router-1(config-if)# mpls traffic-eng tunnels
  router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
```

[If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

## Guaranteed Bandwidth Service Configuration

Having configured two bandwidth pools, you now can

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, it is possible to achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or diffserv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort/diffserv traffic, thereby achieving a greater utilization of those links.

## Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue—or in diffserv terminology, select a PHB (per-hop behavior)—to be used exclusively by the strict guarantee traffic. This shall be called the “GB queue.”

If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. On the Cisco 7500(VIP) it is the "priority" queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used. On the Cisco 7500 (VIP) you use one of the existing Class-Based Weighted Fair Queuing (CBWFQ) queues.

2. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop*, and that no other traffic is placed in this queue.

You do this by marking the traffic that enters the tunnel with a unique value in the mpls exp bits field, and steering only traffic with that marking into the GB queue.

3. Ensure that this GB queue is never oversubscribed; that is, see that no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (in the case of delay/jitter guarantees) or can be marked differently for preferential discard (in the case of bandwidth guarantees).

4. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the *z* parameter of the **ip RSVP bandwidth** command).

## Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct diffserv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (diffserv AF2, AF3, and AF4).
2. Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6).
3. Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of diffserv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

## Providing Strict Guarantees and Differentiated Service in the Same Network

Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and diffserv can be supported simultaneously in a given network.

## Guaranteed Bandwidth Service Examples

Given the many topologies in which Guaranteed Bandwidth Services can be applied, there is space here only to present two examples. They illustrate opposite ends of the spectrum of possibilities.

In the first example, the guaranteed bandwidth tunnel can be easily specified by its destination. So the forwarding criteria refer to a single destination prefix.

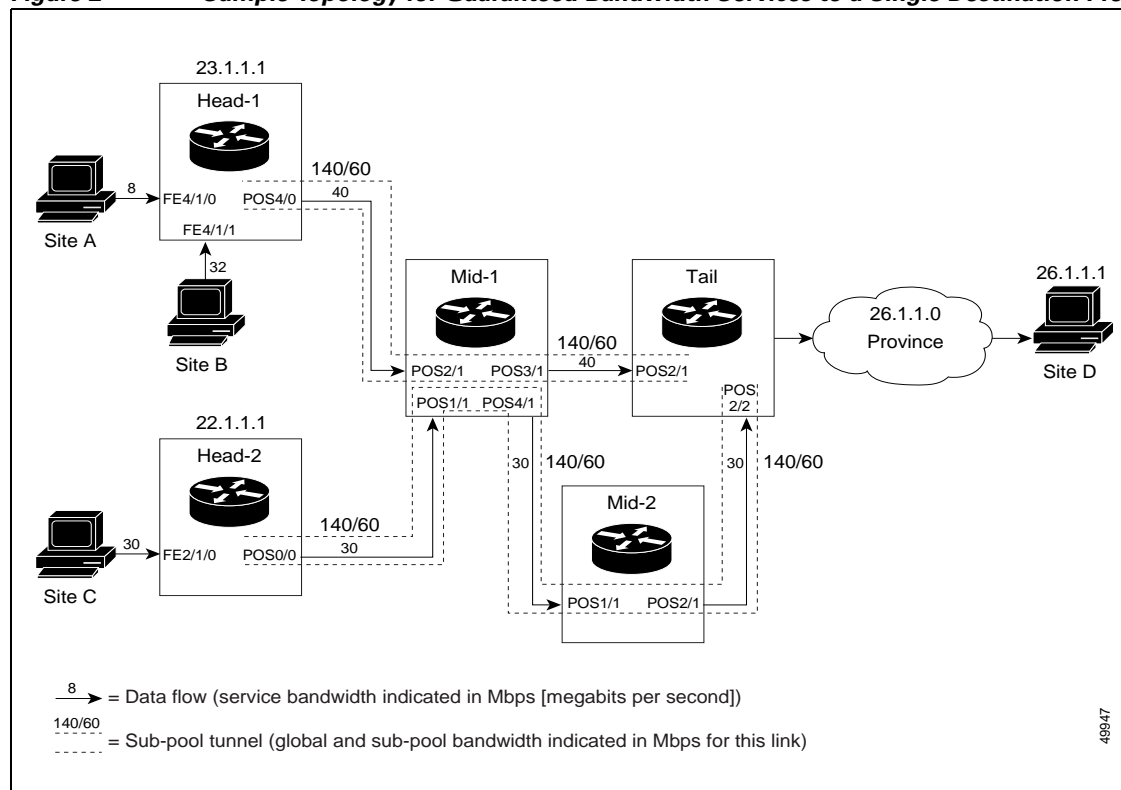
In the second example, there can be many final destinations for the guaranteed bandwidth traffic, including a dynamically changing number of destination prefixes. So the forwarding criteria are specified by Border Gateway Protocol (BGP) policies.

### Example with Single Destination Prefix

**Figure 2 illustrates** a topology for guaranteed bandwidth services whose destination is specified by a single prefix, either Site D (like a voice gateway, here bearing prefix 26.1.1.1) or a subnet (like the location of a web farm, here called “Province” and bearing prefix 26.1.1.0). Three services are offered:

- From Site A (defined as all traffic arriving at interface FE4/1/0): to host 26.1.1.1, 8 Mbps of guaranteed bandwidth with low loss, low delay and low jitter
- From Site B (defined as all traffic arriving at interface FE4/1/1): towards subnet 26.1.1.0, 32 Mbps of guaranteed bandwidth with low loss
- From Site C (defined as all traffic arriving at interface FE2/1/0): 30 Mbps of guaranteed bandwidth with low loss

**Figure 2** Sample Topology for Guaranteed Bandwidth Services to a Single Destination Prefix



These three services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the router-4 tail
- From the Head-2 router, 22.1.1.1, to the router-4 tail

Both tunnels use the same tail router, though they have different heads. (In [Figure 2](#) one midpoint router is shared by both tunnels. In the real world there could of course be many more midpoints.)

All POS interfaces in this example are OC3, whose capacity is 155 Mbps.

## Configuring Tunnel Head-1

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel. (With the 7500 router, Modular QoS CLI is used.)

### Configuring the Pools and Tunnel

At the device level:

```

router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis                                router ospf 100
router-1(config-router)# net                                 redistribute connected
49.0000.1000.0000.0010.00
router-1(config-router)# metric-style wide                    network 10.1.1.0 0.0.0.255 area 0
router-1(config-router)# is-type level-1                      network 23.1.1.1 0.0.0.0 area
  0
router-1(config-router)# mpls traffic-eng                    mpls traffic-eng area 0
level-1
router-1(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit

```

Create a virtual interface:

```

router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit

```

At the outgoing physical interface:

```

router-1(config)# interface pos4/0
router-1(config-if)# ip address 10.1.1.1 255.0.0.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the tunnel interface:

```

router-1(config)# interface Tunnell

```

```

router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic

```

To ensure that packets destined to host 26.1.1.1 and subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```

router-1(config)# ip route 26.1.1.0 255.255.255.0 Tunnel1
router-1(config)# exit

```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```

router-1(config)# no tunnel mpls traffic-eng autoroute announce

```

## For Service from Site A to Site D

At the inbound physical interface (FE4/1/0):

1. In global configuration mode, create a class of traffic matching ACL 100, called "sla-1-class":

```

class-map match-all sla-1-class
  match access-group 100

```

2. Create an ACL 100 to refer to all packets destined to 26.1.1.1:

```

access-list 100 permit ip any host 26.1.1.1

```

3. Create a policy named "sla-1-input-policy", and according to that policy:

- a. Packets in the class called "sla-1-class" are rate-limited to:

– a rate of 8 million bits per second

– a normal burst of 1 million bytes

– a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.

- d. All other packets are marked with experimental bit 0 and are forwarded.

```

policy-map sla-1-input-policy
  class sla-1-class
    police 8000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0

```

4. The policy is applied to packets entering interface FE4/1/0.

```

interface FastEthernet4/1/0
  service-policy input sla-1-input-policy

```

## For Service from Site B to Subnet “Province”

At the inbound physical interface (FE4/1/1):

1. In global configuration mode, create a class of traffic matching ACL 120, called "sla-2-class":

```
class-map match-all sla-2-class
  match access-group 120
```

2. Create an ACL, 120, to refer to all packets destined to subnet 26.1.1.0:

```
access-list 120 permit ip any 26.1.1.0 0.0.0.255
```

3. Create a policy named “sla-2-input-policy”, and according to that policy:

- a. Packets in the class called “sla-2-class” are rate-limited to:

– a rate of 32 million bits per second

– a normal burst of 1 million bytes

– a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.

- d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-2-input-policy
  class sla-2-class
    police 32000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/1/1.

```
interface FastEthernet4/1/1
  service-policy input sla-2-input-policy
```

## For Both Services

The outbound interface (POS4/0) is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
  match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 62 kbits/sec).

```
policy-map output-interface-policy
  class exp-5-traffic
    priority 32
```

3. The policy is applied to packets exiting interface POS4/0.

```
interface POS4/0
  service-policy output output-interface-policy
```

The result of the above configuration lines is that packets entering the Head-1 router via interface FE4/1/0 destined to host 26.1.1.1, or entering the router via interface FE4/1/1 destined to subnet 26.1.1.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the

router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS4/0, will be placed into the priority queue.

**Note**

Packets entering the router via FE4/1/0 or FE4/1/1 and exiting POS4/0 enter as IP packets and exit as MPLS packets.

## Configuring Tunnel Head-2

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service on the sub-pool tunnel.

### Configuring the Pools and Tunnel

At the device level:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> router-2(config)# ip cef distributed router-2(config)# mpls traffic-eng tunnels [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:  router-2(config)# router isis router-2(config-router)# net 49.0000.1000.0000.0011.00 router-2(config-router)# metric-style wide router-2(config-router)# is-type level-1  router-2(config-router)# mpls traffic-eng level-1 router-2(config-router)# passive-interface Loopback0 [now one resumes the common command set]: router-2(config-router)# mpls traffic-eng router-id Loopback0 router-2(config-router)# exit </pre> | <pre> router ospf 100 redistribute connected network 11.1.1.0 0.0.0.255 area 0 network 22.1.1.1 0.0.0.0 area 0 mpls traffic-eng area 0 </pre> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|

Create a virtual interface:

```

router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# no ip directed broadcast
router-2(config-if)# exit

```

At the outgoing physical interface:

```

router-2(config)# interface pos0/0
router-2(config-if)# ip address 11.1.1.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit

```

At the tunnel interface:

```

router-2(config)# interface Tunnel2

```



```

router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-2(config-if)# exit

```

And to ensure that packets destined to subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route, at the device level:

```

router-2(config)# ip route 26.1.1.0 255.255.255.0 Tunnel2
router-2(config)# exit

```

Finally, in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```

router-2(config)# no tunnel mpls traffic-eng autoroute announce

```

### For Service from Site C to Subnet "Province"

At the inbound physical interface (FE2/1/0):

1. In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":

```

class-map match-all sla-3-class
  match access-group 130

```

2. Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:

```

access-list 130 permit ip any 26.1.1.0 0.0.0.255

```

3. Create a policy named "sla-3-input-policy", and according to that policy:

- a. Packets in the class called "sla-3-class" are rate-limited to:

– a rate of 30 million bits per second

– a normal burst of 1 million bytes

– a maximum burst of 2 million bytes

- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.

- d. All other packets are marked with experimental bit 0 and are forwarded.

```

policy-map sla-3-input-policy
  class sla-3-class
    police 30000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0

```

4. The policy is applied to packets entering interface FE2/1/0.

```

interface FastEthernet2/1/0
  service-policy input sla-3-input-policy

```

The outbound interface POS0/0 is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```

class-map match-all exp-5-traffic

```

```
match mpls experimental 5
```

2. Create a policy named “output-interface-policy”. According to that policy, packets in the class “exp-5-traffic” are put in the priority queue (which is rate-limited to 32 kbits/sec).

```
policy-map output-interface-policy
  class exp-5-traffic
    priority 32
```

3. The policy is applied to packets exiting interface POS0/0:

```
interface POS0/0
  service-policy output output-interface-policy
```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1/0 and destined for subnet 26.1.1.0 have their IP precedence field set to 5. It is assumed that no other packets entering this router (on any interface) are using this precedence. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another precedence value.) When exiting this router via interface POS0/0, packets marked with precedence 5 are placed in the priority queue.

**Note**

Packets entering the router via FE2/1/0 and exiting through POS0/0 enter as IP packets and exit as MPLS packets.

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef distributed
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

```
router-3(config)# router isis
```

```
router-3(config-router)# net
49.0000.2400.0000.0011.00
```

```
router-3(config-router)# metric-style wide
```

```
router-3(config-router)# is-type level-1
```

```
router-3(config-router)# mpls traffic-eng
level-1
```

```
router-3(config-router)# passive-interface
Loopback0
```

```
router-3(config-router)#
```

```
router-3(config-router)#
```

[now one resumes the common command set]:

```
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit
```

```
router ospf 100
```

```
redistribute connected
```

```
network 10.1.1.0 0.0.0.255 area 0
```

```
network 11.1.1.0 0.0.0.255
area 0
```

```
network 24.1.1.1 0.0.0.0 area
0
```

```
network 12.1.1.0 0.0.0.255 area 0
```

```
network 13.1.1.0 0.0.0.255 area 0
```

```
mpls traffic-eng area 0
```

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit

```

At the physical interface level (ingress):

```

router-3(config)# interface pos2/1
router-3(config-if)# ip address 10.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 11.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress):

```

router-3(config)# interface pos3/1
router-3(config-if)# ip address 12.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos4/1
router-3(config-if)# ip address 13.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnel

At the device level:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <pre> router-5(config)# ip cef distributed router-5(config)# mpls traffic-eng tunnels [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:  router-5(config)# router isis                                 router ospf 100                                 redistribute connected router-5(config-router)# net                                 49.2500.1000.0000.0012.00                                 49.2500.1000.0000.0012.00 </pre> |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

```

router-5(config-router)# metric-style wide
router-5(config-router)# is-type level-1

router-5(config-router)# mpls traffic-eng
level-1
router-5(config-router)# passive-interface
Loopback0
[now one resumes the common command set]:

router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit

```

```

network 13.1.1.0 0.0.0.255 area 0
network 14.1.1.0 0.0.0.255
area 0
network 25.1.1.1 0.0.0.0 area
0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit

```

At the physical interface level (ingress):

```

router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit

```

At the physical interface level (egress):

```

router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit

```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured identically to the inbound interfaces of the midpoint routers (except, of course, for the ID of each particular interface):

### Configuring the Pools and Tunnels

At the device level:

```

router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-4(config)# router isis
router-4(config-router)# net
49.0000.2700.0000.0000.00
router-4(config-router)# metric-style wide

```

```

router ospf 100
redistribute connected
network 12.1.1.0 0.0.0.255 area 0

```

```

router-4(config-router)# is-type level-1
router-4(config-router)# mpls traffic-eng level-1
router-4(config-router)# passive-interface Loopback0
[now one resumes the common command set]:
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# exit

```

```

network 14.1.1.0 0.0.0.255
area 0
network 27.1.1.1 0.0.0.0 area
0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit

```

At the physical interface (ingress):

```

router-4(config)# interface pos2/1
router-4(config-if)# ip address 12.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 14.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

```

Because the tunnel ends on the tail (does not include any outbound interfaces of the tail router), no outbound QoS configuration is used.

## Example with Many Destination Prefixes

Figure 3 illustrates a topology for guaranteed bandwidth services whose destinations are a set of prefixes. Those prefixes usually share some common properties such as belonging to the same Autonomous System (AS) or transiting through the same AS. Although the individual prefixes may change dynamically because of route flaps in the downstream autonomous systems, the properties the prefixes share will not change. Policies addressing the destination prefix set are enforced through Border Gateway Protocol (BGP), which is described in the following documents:

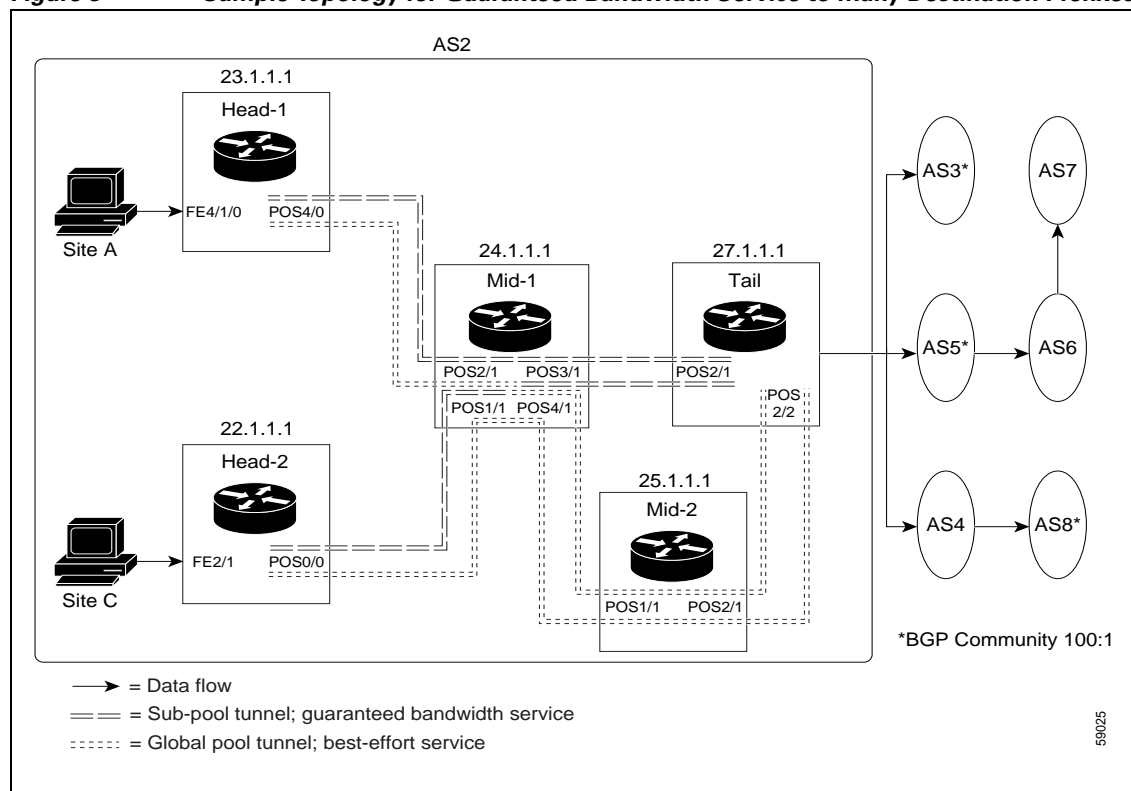
- “Configuring QoS Policy Propagation via Border Gateway Protocol” in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_c/qcprt1/qcdprop.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt1/qcdprop.htm))
- “Configuring BGP” in the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt2/1cdbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdbgp.htm))

- “BGP Commands” in the *Cisco IOS IP and IP Routing Command Reference*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_r/1rprpt2/1rdbgp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/1rprpt2/1rdbgp.htm))
- “BGP-Policy Command” in the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.1 ([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_r/qrdcmd1.htm#xtocid89313](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/qrdcmd1.htm#xtocid89313))

In this example, three guaranteed bandwidth services are offered, each coming through a 7500 or a 12000 edge device:

- Traffic coming from Site A (defined as all traffic arriving at interface FE4/1/0) and from Site C (defined as all traffic arriving at interface FE2/1) destined to AS5
- Traffic coming from Sites A and C that transits AS5 but is not destined to AS5. (In the figure, the transiting traffic will go to AS6 and AS7)
- Traffic coming from Sites A and C destined to prefixes advertised with a particular BGP community attribute (100:1). In this example, Autonomous Systems #3, #5, and #8 are the BGP community assigned the attribute 100:1.

**Figure 3 Sample Topology for Guaranteed Bandwidth Service to Many Destination Prefixes**



The applicability of guaranteed bandwidth service is not limited to the three types of multiple destination scenarios described above. There is not room in this document to present all possible scenarios. These three were chosen as representative of the wide range of possible deployments.

The guaranteed bandwidth services run through two sub-pool tunnels:

- From the Head-1 router, 23.1.1.1, to the tail

- From the Head-2 router, 22.1.1.1, to that same tail

In addition, a global pool tunnel has been configured from each head end, to carry best-effort traffic to the same destinations. All four tunnels use the same tail router, even though they have different heads and differ in their passage through the midpoints. (Of course in the real world there would be many more midpoints than just the two shown here.)

All POS interfaces in this example are OC3, whose capacity is 155 Mbps.

Configuring a multi-destination guaranteed bandwidth service involves:

- Building a sub-pool MPLS-TE tunnel
- Configuring DiffServ QoS
- Configuring QoS Policy Propagation via BGP (QPPB)
- Mapping traffic onto the tunnels

All of these tasks are included in the following example.

## Configuration of Tunnel Head-1

First we recapitulate commands that establish a sub-pool tunnel (commands presented earlier on page 13) and now we also configure a global pool tunnel. Additionally, we present QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (With the 7500(VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

```
router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis                                router ospf 100
router-1(config-router)# net                                 redistribute connected
49.0000.1000.0000.0010.00                                    network 10.1.1.0 0.0.0.255 area 0
router-1(config-router)# metric-style wide                    network 23.1.1.1 0.0.0.0 area
router-1(config-router)# is-type level-1                      0
  mpls traffic-eng area 0

router-1(config-router)# mpls traffic-eng
level-1
[now one resumes the common command set]:

router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# exit
```

At the outgoing physical interface:

```
router-1(config)# interface pos4/0
router-1(config-if)# ip address 10.1.1.1 255.0.0.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
```

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path1
router-1(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-1(config)# interface Tunnel2
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth 80000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path1
router-1(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-1(config)# ip explicit-path name gbs-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
router-1(config)# ip explicit-path name best-effort-path1
router-1(config-ip-expl-path)# next-address 24.1.1.1
router-1(config-ip-expl-path)# next-address 25.1.1.1
router-1(config-ip-expl-path)# next-address 27.1.1.1
router-1(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE4/1/0), packets received are rate-limited to:

- a rate of 30 Mbps
- a normal burst of 1 MB
- a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-1(config)# interface FastEthernet4/1/0
router-1(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-1(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```



At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```
router-1(config)# class-map match-all exp5-class
router-1(config-cmap)# match mpls experimental 5
router-1(config-cmap)# exit
```

Create a policy that creates a priority queue for “exp5-class”:

```
router-1(config)# policy-map core-out-policy
router-1(config-pmap)# class exp5-class
router-1(config-pmap-c)# priority 100000
router-1(config-pmap-c)# exit
router-1(config-pmap)# class class-default
router-1(config-pmap-c)# bandwidth 55000
router-1(config-pmap-c)# exit
router-1(config-pmap)# exit
```

The policy is applied to packets exiting the outbound interface POS4/0.

```
router-1(config)# interface POS4/0
router-1(config-if)# service-policy output core-out-policy
```

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-1(config)# ip bgp-community new-format
router-1(config)# router bgp 2
router-1(config-router)# no synchronization
router-1(config-router)# table-map set-qos-group
router-1(config-router)# bgp log-neighbor-changes
router-1(config-router)# neighbor 27.1.1.1 remote-as 2
router-1(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-1(config-router)# no auto-summary
router-1(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 so they will be mapped onto Tunnel #1 (the guaranteed bandwidth service tunnel). At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 100
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 101
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
```

```
router-1(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match community 20
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 29.1.1.1
router-1(config-route-map)# exit
router-1(config)# ip community-list 20 permit 100:1
```

### Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #1:

```
router-1(config)# ip route 29.1.1.1 255.255.255.255 Tunnel1
```

Map all best-effort traffic onto Tunnel #2:

```
router-1(config)# ip route 30.1.1.1 255.255.255.255 Tunnel2
```

## Configuration of Tunnel Head-2

As with the Head-1 device and interfaces, the following Head-2 configuration first presents commands that establish a sub-pool tunnel (commands presented earlier on page 13) and then also configures a global pool tunnel. After that it presents QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (Because this is a 7500 (VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

|                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-2(config)# ip cef distributed router-2(config)# mpls traffic-eng tunnels [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:  router-2(config)# router isis router-2(config-router)# net 49.0000.1000.0000.0011.00 router-2(config-router)# metric-style wide router-2(config-router)# is-type level-1  router-2(config-router)# mpls traffic-eng level-1</pre> | <pre>router ospf 100 redistribute connected network 11.1.1.0 0.0.0.255 area 0 network 22.1.1.1 0.0.0.0 area 0 mpls traffic-eng area 0</pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
```

```
router-2(config-if)# exit
```

At the outgoing physical interface:

```
router-2(config)# interface pos0/0
router-2(config-if)# ip address 11.1.1.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-2(config)# interface Tunnel3
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name gbs-path2
router-2(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-2(config)# interface Tunnel4
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth 70000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path2
router-2(config-if)# exit
```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```
router-2(config)# ip explicit-path name gbs-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
router-2(config)# ip explicit-path name best-effort-path2
router-2(config-ip-expl-path)# next-address 24.1.1.1
router-2(config-ip-expl-path)# next-address 25.1.1.1
router-2(config-ip-expl-path)# next-address 27.1.1.1
router-2(config-ip-expl-path)# exit
```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE2/1), packets received are rate-limited to:

- a. a rate of 30 Mbps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```
router-2(config)# interface FastEthernet2/1
router-2(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-2(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit
```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```
router-2(config)# class-map match-all exp5-class
router-2(config-cmap)# match mpls experimental 5
router-2(config-cmap)# exit
```

Create a policy that creates a priority queue for “exp5-class”:

```
router-2(config)# policy-map core-out-policy
router-2(config-pmap)# class exp5-class
router-2(config-pmap-c)# priority 100000
router-2(config-pmap-c)# exit
router-2(config-pmap)# class class-default
router-2(config-pmap-c)# bandwidth 55000
router-2(config-pmap-c)# exit
router-2(config-pmap)# exit
```

The policy is applied to packets exiting interface POS0/0:

```
interface POS0/0
 service-policy output core-out-policy
```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1 and destined for AS5, BGP community 100:1, or transiting AS5 will have their experimental field set to 5. It is assumed that no other packets entering this router (on any interface) are using this exp bit value. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another experimental value.) When exiting this router via interface POS0/0, packets marked with experimental value 5 are placed into the priority queue.



#### Note

Packets entering the router via FE2/1 and exiting through POS0/0 enter as IP packets and exit as MPLS packets.

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-2(config)# ip bgp-community new-format
router-2(config)# router bgp 2
router-2(config-router)# no synchronization
router-2(config-router)# table-map set-qos-group
router-2(config-router)# bgp log-neighbor-changes
router-2(config-router)# neighbor 27.1.1.1 remote-as 2
router-2(config-router)# neighbor 27.1.1.1 update-source Loopback0
router-2(config-router)# no auto-summary
router-2(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 so they will be mapped onto Tunnel #3 (the guaranteed bandwidth service tunnel). At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 100
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 101
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match community 20
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 29.1.1.1
router-2(config-route-map)# exit
router-2(config)# ip community-list 20 permit 100:1
```

### Mapping the Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #3:

```
router-2(config)# ip route 29.1.1.1 255.255.255.255 Tunnel3
```

Map all best-effort traffic onto Tunnel #4:

```
router-2(config)# ip route 30.1.1.1 255.255.255.255 Tunnel4
```

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured very much like the outbound interface of the head router. The strategy is to have all mid-point routers in this Autonomous System ready to carry future as well as presently configured sub-pool and global pool tunnels.

### Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef distributed
```

router-3(config)# **mpls traffic-eng tunnels**  
 [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> router-3(config)# <b>router isis</b> router-3(config-router)# <b>net</b> <b>49.0000.2400.0000.0011.00</b> router-3(config-router)# <b>metric-style wide</b> router-3(config-router)# <b>is-type level-1</b>  router-3(config-router)# <b>mpls traffic-eng</b> <b>level-1</b> router-3(config-router)# router-3(config-router)# router-3(config-router)# router-3(config-router)# </pre> | <pre> router ospf 100 redistribute connected network 10.1.1.0 0.0.0.255 area 0 network 11.1.1.0 0.0.0.255 area 0 network 24.1.1.1 0.0.0.0 area 0 network 12.1.1.0 0.0.0.255 area 0 network 13.1.1.0 0.0.0.255 area 0 mpls traffic-eng area 0 </pre> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set]:

```

router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit

```

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# exit

```

At the physical interface level (ingress):

```

router-3(config)# interface pos2/1
router-3(config-if)# ip address 10.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 11.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress), through which two sub-pool tunnels currently exit:

```

router-3(config)# interface pos3/1
router-3(config-if)# ip address 12.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress), through which two global pool tunnels currently exit:

```

router-3(config)# interface pos4/1
router-3(config-if)# ip address 13.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000

```

```
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on this midpoint router are configured like the outbound interfaces of the Mid-1 router.

### Configuring the Pools and Tunnels

At the device level:

```
router-5(config)# ip cef distributed
router-5(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

|                                                   |                                   |
|---------------------------------------------------|-----------------------------------|
| router-5(config)# <b>router isis</b>              | router ospf 100                   |
| router-5(config-router)# <b>net</b>               | redistribute connected            |
| <b>49.2500.1000.0000.0012.00</b>                  |                                   |
| router-5(config-router)# <b>metric-style wide</b> | network 13.1.1.0 0.0.0.255 area 0 |
| router-5(config-router)# <b>is-type level-1</b>   | network 14.1.1.0 0.0.0.255        |
|                                                   | area 0                            |
| router-5(config-router)# <b>mpls traffic-eng</b>  | network 25.1.1.1 0.0.0.0 area     |
| <b>level-1</b>                                    | 0                                 |
| router-5(config-router)#                          | mpls traffic-eng area 0           |

[now one resumes the common command set]:

```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# exit
```

At the physical interface level (ingress):

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

At the physical interface level (egress):

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured much like the outbound interfaces of the midpoint routers:

### Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right. In the case of OSPF, one must advertise two new loopback interfaces—29.1.1.1 and 30.1.1.1 in our example—which are defined in the QoS Policy Propagation section, further along on this page]:

|                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>router-4(config)# router isis router-4(config-router)# net 49.0000.2700.0000.0000.00 router-4(config-router)# metric-style wide router-4(config-router)# is-type level-1  router-4(config-router)# mpls traffic-eng level-1  router-4(config-router)#  router-4(config-router)#  router-4(config-router)#</pre> | <pre>router ospf 100 redistribute connected  network 12.1.1.0 0.0.0.255 area 0 network 14.1.1.0 0.0.0.255 area 0 network 27.1.1.1 0.0.0.0 area 0 network 29.1.1.1 0.0.0.0 area 0 network 30.1.1.1 0.0.0.0 area 0  mpls traffic-eng area 0</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

[now one resumes the common command set, taking care to include the two additional loopback interfaces]:

```
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng router-id Loopback1
router-4(config-router)# mpls traffic-eng router-id Loopback2
router-4(config-router)# exit
```

Create a virtual interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# exit
```

At the physical interface (ingress):

```
router-4(config)# interface pos2/1
router-4(config-if)# ip address 12.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 14.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
```



```
[and in all cases]:  
router-4(config-if)# exit
```

## Configuring QoS Policy Propagation

On the tail device, one must configure a separate virtual loopback IP address for each class-of-service terminating here. The headend routers need these addresses to map traffic into the proper tunnels. In the current example, four tunnels terminate on the same tail device but they represent only two service classes, so only two additional loopback addresses are needed:

Create two virtual interfaces:

```
router-4(config)# interface Loopback1  
router-4(config-if)# ip address 29.1.1.1 255.255.255.255  
[and if using IS-IS instead of OSPF]:  
router-4(config-if)# ip router isis  
[and in all cases]:  
router-4(config-if)# exit  
router-4(config)# interface Loopback2  
router-4(config-if)# ip address 30.1.1.1 255.255.255.255  
[and if using IS-IS instead of OSPF]:  
router-4(config-if)# ip router isis  
[and in all cases]:  
router-4(config-if)# exit
```

At the device level, configure BGP to send the community to each tunnel head:

```
router-4(config)# ip bgp-community new-format  
router-4(config)# router bgp 2  
router-4(config-router)# neighbor 23.1.1.1 send-community  
router-4(config-router)# neighbor 22.1.1.1 send-community  
router-4(config-router)# exit
```

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **ip rsvp bandwidth**
- **mpls traffic-eng ds-te bc-model**
- **mpls traffic-eng ds-te mode**
- **show mpls traffic-eng topology**
- **tunnel mpls traffic-eng bandwidth**

# Glossary

This section defines acronyms and words that may not be readily understood.

**AS**—Autonomous System. A collection of networks under a common administration, sharing a common routing strategy and identified by a unique 16-bit number (assigned by the Internet Assigned Numbers Authority).

**BGP**—Border Gateway Protocol. The predominant interdomain routing protocol. It is defined by RFC 1163. Version 4 uses route aggregation mechanisms to reduce the size of routing tables.

**CBR**—Constraint Based Routing. The computation of traffic paths that simultaneously satisfy label-switched path attributes and current network resource limitations.

**CEF**—Cisco Express Forwarding. A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**CLI**—Command Line Interface. Cisco's interface for configuring and managing its routers.

**DS-TE**—Diff Serv-aware Traffic Engineering. The capability to configure two bandwidth pools on each link, a *global pool* and a *sub-pool*. MPLS traffic engineering tunnels using the sub-pool bandwidth can be configured with Quality of Service mechanisms to deliver guaranteed bandwidth services end-to-end across the network. Simultaneously, tunnels using the global pool can convey DiffServ traffic.

**flooding**—A traffic passing technique used by switches and bridges in which traffic received on an interface is sent out through all of the interfaces of that device except the interface on which the information was originally received.

**GB queue**—Guaranteed Bandwidth queue. A per-hop behavior (PHB) used exclusively by the strict guarantee traffic. If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used.

**Global Pool**—The total bandwidth allocated to an MPLS traffic engineering link.

**IGP**—Interior Gateway Protocol. An internet protocol used to exchange routing information within an autonomous system. Examples of common internet IGP include IGRP, OSPF, and RIP.

**label-switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**IS-IS**—Intermediate System-to-Intermediate System. A link-state hierarchical routing protocol, based on DECnet Phase V routing, whereby nodes exchange routing information based on a single metric, to determine network topology.

**LCAC**—Link-level (per-hop) call admission control.

**LSP**—Label-switched path (see above).

*Also* Link-state packet—A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSPs are used by the receiving routers to maintain their routing tables. Also called link-state advertisement (LSA).

**MPLS**—Multi-Protocol Label Switching (formerly known as Tag Switching). A method for directing packets primarily through Layer 2 switching rather than Layer 3 routing, by assigning the packets short fixed-length labels at the ingress to an MPLS cloud, using the concept of forwarding equivalence classes. Within the MPLS domain, the labels are used to make forwarding decisions mostly without recourse to the original packet headers.

**MPLS TE**—MPLS Traffic Engineering (formerly known as “RRR” or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

**OSPF**—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**RSVP**—Resource reSerVation Protocol. An IETF protocol used for signaling requests (to set aside internet services) by a customer before that customer is permitted to transmit data over that portion of the network.

**Sub-pool**—The more restrictive bandwidth in an MPLS traffic engineering link. The sub-pool is a portion of the link's overall global pool bandwidth.

**TE**—Traffic engineering. The application of scientific principles and technology to measure, model, and control internet traffic in order to simultaneously optimize traffic performance and network resource utilization.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



## **MPLS Traffic Engineering: Path, Link, and Node Protection**





# MPLS Traffic Engineering: Inter-AS TE

---

**First Published: August 09, 2004**

**Last Updated: July 11, 2008**

The MPLS Traffic Engineering: Inter-AS TE feature provides Autonomous System Boundary Router (ASBR) node protection, loose path reoptimization, stateful switchover (SSO) recovery of label-switched paths (LSPs) that include loose hops, ASBR forced link flooding, Cisco IOS Resource Reservation Protocol (RSVP) local policy extensions for interautonomous system (Inter-AS), and per-neighbor keys:

- ASBR node protection—Protects interarea and Inter-AS TE label-switched paths (LSPs) from the failure of an Area Border Router (ABR) or ASBR.
- Loose path reoptimization—Allows a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel's LSPs to traverse hops that are not in the tunnel headend router's topology database (that is, they are not in the same Open Shortest Path First (OSPF) area, Intermediate System-to-Intermediate System (IS-IS) level, or autonomous system as the tunnel's headend router).
- Loose hop recovery—Supports SSO recovery of LSPs that include loose hops.
- ASBR forced link flooding—Helps an LSP cross a boundary into another domain when information in the other domain is not available to the headend router.
- Cisco IOS RSVP local policy extensions for Inter-AS—Allows network administrators to create controlled policies for TE tunnels that function across multiple autonomous systems.
- Per-neighbor keys—Allows cryptographic authentication to be accomplished on a per-neighbor basis.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS Traffic Engineering: Inter-AS TE”](#) section on [page 27](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for MPLS Traffic Engineering: Inter-AS TE, page 2](#)
- [Restrictions for MPLS Traffic Engineering: Inter-AS TE, page 2](#)
- [Information About MPLS Traffic Engineering: Inter-AS TE, page 3](#)
- [How to Configure MPLS Traffic Engineering: Inter-AS TE, page 11](#)
- [Configuration Examples for MPLS Traffic Engineering: Inter-AS TE, page 21](#)
- [Additional References, page 25](#)
- [Command Reference, page 26](#)
- [Feature Information for MPLS Traffic Engineering: Inter-AS TE, page 27](#)
- [Glossary, page 28](#)

## Prerequisites for MPLS Traffic Engineering: Inter-AS TE

- Enable MPLS.
- Configure TE on routers.
- Ensure that your network supports the following Cisco IOS features:
  - MPLS
  - Cisco Express Forwarding
  - IS-IS or OSPF
- For loose path reoptimization, know how to configure the following:
  - IP explicit paths for MPLS TE tunnels
  - Loose hops
  - Interarea and Inter-AS tunnels

## Restrictions for MPLS Traffic Engineering: Inter-AS TE

### Loose Path Reoptimization

- Midpoint reoptimization is not supported.

### ASBR Forced Link Flooding

- The TE metric and affinity attributes that are known at a headend router (and used as constraints when an LSP's path is computed) are not currently signaled. Consequently, explicit router (ERO) expansions do not consider these constraints.
- Each node in an autonomous system must have a unique router ID.
- The router ID configured on a link must not conflict with the router ID within the autonomous system.



- If a link is configured for forced link flooding, the link's neighbors are not learned by regular Interior Gateway Protocol (IGP) updates. If a link is already learned about neighbors by IGP on a link, you cannot configure the link as passive. Therefore, to configure a link for forced flooding, be sure that the node does not already have a neighbor on that link.

## Information About MPLS Traffic Engineering: Inter-AS TE

To configure the MPLS Traffic Engineering: Inter-AS TE feature, you need to understand the following concepts:

- [MPLS Traffic Engineering Tunnels, page 3](#)
- [Multiarea Network Design, page 3](#)
- [Fast Reroute, page 4](#)
- [ASBR Node Protection, page 4](#)
- [Loose Path Reoptimization, page 7](#)
- [ASBR Forced Link Flooding, page 9](#)
- [Link Flooding, page 11](#)

## MPLS Traffic Engineering Tunnels

MPLS TE lets you build LSPs across your network that you then forward traffic down.

MPLS TE LSPs, also called TE tunnels, let the headend of a TE tunnel control the path its traffic takes to a particular destination. This method is more flexible than forwarding traffic based only on a destination address.

Interarea tunnels allow you to do the following:

- Build TE tunnels between areas (interarea tunnels)
- Build TE tunnels that start and end in the same area, on multiple areas on a router (intra-area tunnels)

Some tunnels are more important than others. For example, you may have tunnels carrying Voice over IP (VoIP) traffic and tunnels carrying data traffic that are competing for the same resources. Or you may simply have some data tunnels that are more important than others. MPLS TE allows you to have some tunnels preempt others. Each tunnel has a priority, and more-important tunnels take precedence over less-important tunnels.

## Multiarea Network Design

You can establish MPLS TE tunnels that span multiple IGP areas and levels. The tunnel headend routers and tailend routers do not have to be in the same area. The IGP can be either IS-IS or OSPF.

To configure an interarea tunnel, use the **next-address loose** command to specify on the headend router a loosely routed explicit path of the LSP that identifies each ABR the LSP should traverse. The headend router and the ABRs along the specified explicit path expand the loose hops, each computing the path segment to the next ABR or tunnel destination.

## Fast Reroute

MPLS Fast Reroute (FRR) is a fast recovery local protection technique that protects TE LSPs from link, shared risk link group (SRLG), and node failure. One or more TE LSPs (called backup LSPs) are preestablished to protect against the failure of a link, node, or SRLG. If there is a failure, each protected TE LSP traversing the failed resource is rerouted onto the appropriate backup tunnels.

The backup tunnel must meet the following requirements:

- It should not pass through the element it protects.
- It should intersect with a primary tunnel at a minimum of two nodes: point of local repair (PLR) and merge point (MP). The PLR should be the headend LSR of the backup tunnel, and the MP should be the tailend LSR of the backup tunnel. The PLR is where FRR is triggered when a link, node, or SRLG failure occurs.
- FRR protection can be performed for an Inter-AS tunnel only if the backup tunnel's merge point can route packets to the PLR's backup tunnel's egress interface. You can configure a static route or you can configure Border Gateway Protocol (BGP) to export the backup tunnel's egress interface to other autonomous systems.
- If the preferred link is a passive link, you must assign an administrative-weight for it. To assign an administrative weight, use the **mpls traffic-eng administrative-weight** command in interface configuration mode.
- Each router must be configured with the **mpls traffic-eng reoptimize events link-up** command in global configuration mode.

## ASBR Node Protection

A TE LSP that traverses an ASBR needs a special protection mechanism (ASBR node protection) because the MP and PLR will be in different autonomous systems that have different IGPs.

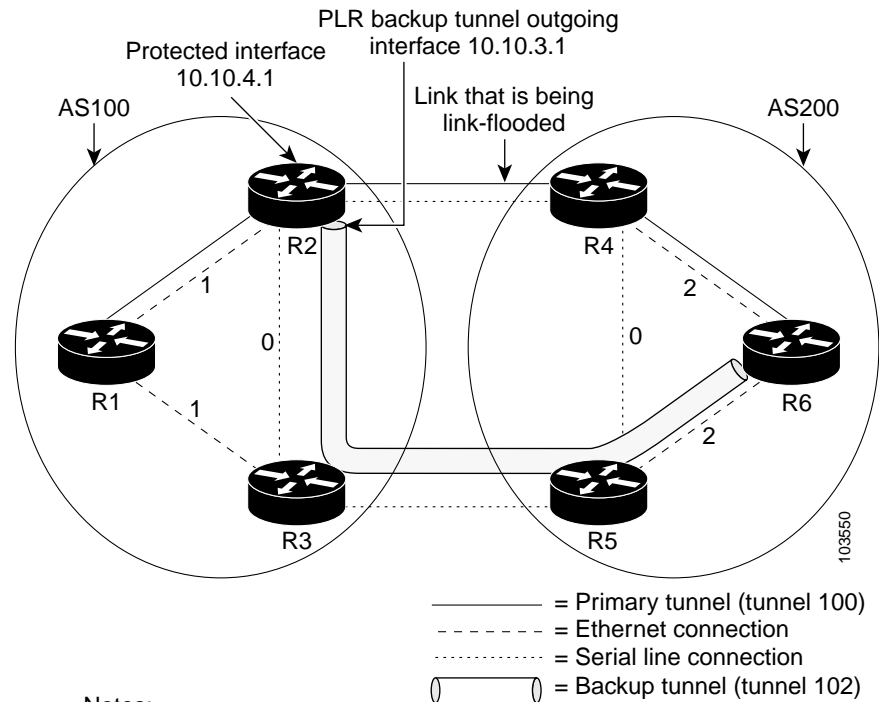
A PLR ensures that the backup tunnel intersects with the primary tunnel at the MP by examining the Record Route Object (RRO) of the primary tunnel to see if any addresses specified in the RRO match the destination of the backup tunnel.

Addresses specified in RRO IPv4 and IPv6 subobjects can be node-IDs and interface addresses. The traffic engineering RFC 3209 specifies that you can use a router address or interface address, but recommends using the interface address of outgoing path messages. Therefore, in [Figure 1](#) router R2 is more likely to specify interface addresses in the RRO objects carried in the resv messages of the primary tunnel (T1) and the backup tunnel.

Node IDs allow the PLR to select a suitable backup tunnel by comparing node IDs in the resv RRO to the backup tunnel's destination.

RSVP messages that must be routed and forwarded to the appropriate peer (for example, an resv message) require a route from the MP back to the PLR for the RSVP messages to be delivered. The MP needs a route to the PLR backup tunnel's outgoing interface for the resv message to be delivered. Therefore, you must configure a static route from the MP to the PLR. For the configuration procedure, see the [“Configuring a Static Route from the MP to the PLR”](#) section on page 14.

[Figure 1](#) illustrates ASBR node protection. Router R4 is node-protected with a backup tunnel from R2-R3-R5-R6.

**Figure 1 ASBR Node Protection****Notes:**

There are two autonomous systems.  
 The numbers within the Ethernet serial connection indicate the OSPF area number.  
 There is no IGP between R2 and R4, and R3 and R5.

In this configuration, IP addresses are as follows:

- R1—Loopback0 10.10.0.1
  - Ethernet 0—IP address of 10.10.1.1 is connected to R2 Ethernet 0
  - Ethernet 1—IP address of 10.10.2.1 is connected to R3 Ethernet 1
- R2—Loopback0 10.10.0.2
  - Ethernet 0—IP address of 10.10.1.2 is connected to R1 Ethernet 0
  - Ethernet 1—IP address of 10.10.3.1 is connected to R3 Ethernet 1
  - Serial 2—IP address of 10.10.4.1 is connected to R4 serial 2
- R3—Loopback0 10.10.0.3
  - Ethernet 0—IP address of 10.10.2.2 is connected to R1 Ethernet 1
  - Ethernet 1—IP address of 10.10.3.2 is connected to R2 Ethernet 1
  - Serial 2—IP address of 10.10.5.1 is connected to R5 serial 2
- R4—Loopback0 10.10.0.4
  - Ethernet 0—IP address of 10.10.7.1 is connected to R6 Ethernet 0
  - Ethernet 1—IP address of 10.10.6.1 is connected to R5 Ethernet 1
  - Serial 2—IP address of 10.10.4.2 is connected to R2 serial 2
- R5—Loopback0 10.10.0.5

- Ethernet 0—IP address of 10.10.8.1 is connected to R6 Ethernet 0
- Ethernet 1—IP address of 10.10.6.2 is connected to R4 Ethernet 1
- Serial 2—IP address of 10.10.5.2 is connected to R3 serial 2
- R6—Loopback0 10.10.0.6
  - Ethernet 0—IP address of 10.10.7.2 is connected to R4 Ethernet 0
  - Ethernet 1—IP address of 10.10.8.2 is connected to R5 Ethernet 1

In [Figure 1](#), the following situations exist:

- Routers R1, R2, and R3 are in AS 100. The R1-R2 and R1-R3 links are in OSPF area 1.
- Routers R4, R5, and R6 are in AS200. The R4-R6 and R5-R6 links are in OSPF area 2.
- The link R2-R3 is in AS100, and link R4-R5 is in AS200. The links R2-R3 and R4-R5 are in OSPF area 0.
- The links R2-R4 and R3-R5 are not running an IGP because they cross the Inter-AS boundary between AS100 and AS200. Because they are not running IGP, you must configure an administrative weight for each passive interface for FRR to work. Use the **mpls traffic-eng administrative-weight** command in interface configuration mode.
- There is a primary tunnel, tunnel 100, from R1-R2-R4-R6.
- There is a backup tunnel, tunnel 102, from R2-R3-R5-R6.
- There is a TE tunnel, tunnel 101, from R6-R5-R3-R1 for returning data traffic for tunnel 100.
- There is a TE tunnel, tunnel 103, from R6-R5-R3-R2 for returning data traffic for tunnel 102.
- The explicit paths of all the tunnels use loose hops.
- The R2-R4 link is configured to be link flooded in both R2's and R4's IGP. The R3-R5 link is configured to be link flooded in both R3's and R5's IGP.

Router R2 needs to ensure the following:

- Backup tunnel intersects with the primary tunnel at the MP, and therefore has a valid MP address. In [Figure 1](#), R2 needs to determine that tunnel 100 and backup tunnel 102 share MP node R6.
- Backup tunnel satisfies the request of the primary LSP for bandwidth protection. For example, the amount of bandwidth guaranteed for the primary tunnel during a failure, and the type of protection (preferably protecting against a node failure rather than a link failure).

### Node-IDs Signaling in RROs

ASBR node protection includes a node-ID flag (0x20), which is also called a node-ID subobject. When it is set, the flag indicates that the address specified in the RRO object in the resv message is the node-ID address. The node-ID address refers to the traffic engineering router ID.

A node must always use the same address in the RRO (that is, it must use IPv4 or IPv6, but not both).

To display all the hops, enter the following command on the headend router. Sample command output is as follows:

```
Router(config)# show ip rsvp reservations detail
```

```
Reservation:
```

```
Tun Dest: 10.10.0.6 Tun ID: 100 Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1 LSP ID: 31
Next Hop: 10.10.1.2 on Ethernet0/0
Label: 17 (outgoing)
Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
Average Bitrate is 10K bits/sec, Maximum Burst is 1K bytes
```

```

Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
RRO:
  10.10.0.2/32, Flags:0x29 (Local Prot Avail/to NNHOP, Is Node-id)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 17
  10.10.0.4/32, Flags:0x20 (No Local Protection, Is Node-id)
  10.10.7.1/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 17
  10.10.0.6/32, Flags:0x20 (No Local Protection, Is Node-id)
  10.10.7.2/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 0
Resv ID handle: 0100040E.
Status:
Policy: Accepted. Policy source(s): MPLS/TE

```

For a description of the fields, see the *Cisco IOS Quality of Service Solutions Command Reference*.

### Addition of the Node-ID Subobject

When a fast reroutable LSP is signaled, the following actions occur:

- An LSR adds a node-ID subobject and an incoming label subobject in the resv message.
- If there is an RRO object in the path message, an LSR adds a node-ID subobject, an RRO IPv4 subobject that records the interface address, and an incoming label subobject in the resv message.

If you enable record-route on the headend LSR, the interface addresses for the LSP are included in the RRO object of the resv message.

To enable record-route, enter the following command with the **record-route** keyword:

```
tunnel mpls traffic-eng record-route
```

### Processing of an RRO with Node-ID Subobjects

The node-ID subobject is added to the RECORD\_ROUTE object before the label route subobject. If RECORD\_ROUTE is turned on, the RRO object consists of the following in this order: node-ID, interface address, and label.

### Merge Point Location

The destination of the backup tunnel is the node-ID of the MP. A PLR can find the MP and appropriate backup tunnel by comparing the destination address of the backup tunnel with the node-ID subobjects included in the resv RRO for the primary tunnel.

When both the IPv4 node-ID and IPv6 node-ID subobjects are present, a PLR can use either or both of them to find the MP address.

### Determination of Backward Compatibility

To remain compatible with nodes that do not support RRO IPv4 or IPv6 node-ID subobjects, a node can ignore those objects. Those nodes cannot be the MP in a network with interarea or Inter-AS traffic engineering.

## Loose Path Reoptimization

### Interarea and Inter-AS LSPs

If the LSP of an MPLS TE tunnel traverses hops that are not in the headend router's topology database (that is, the hops are in a different OSPF area or IS-IS level), the LSP is called an *interarea TE LSP*.

If the LSP of the tunnel traverses hops that are in a different autonomous system (AS) from the tunnel's headend router, the LSP is called an *Inter-AS TE LSP*.

Interarea LSPs and Inter-AS TE LSPs can be signaled using loose hop subobjects in their EROs. The headend does not have “strict” knowledge of hops beyond its area, so the LSP's path is “loosely” specified at the headend. Downstream routers processing these loose hop subobjects (which do have the knowledge) are relied upon to expand them into strict hops.

### Loose Hop Configuration

Beyond the headend area, configure hops as loose hops. Typically you specify only the ABRs and the tailend router of a tunnel, but any other combination is allowed.

### Loose Hop Expansion

Loose hop expansion is the conversion of a single ERO loose hop subobject into one or more strict hop subobjects.

Interarea and Inter-AS TE LSPs can be signaled using loose hop subobjects in their EROs. When a router receives a path message containing an ERO that has a loose hop as the next address, the router typically expands the ERO by converting the single loose hop subobject into one or more strict hop subobjects. The router typically has the knowledge, in its topology database, of the best way to reach the loose hop and computes this path by using constraint-based shortest path first (CSPF). So the router substitutes this more specific information for the loose hop subobject found in the ERO. This process is called loose hop expansion or ERO expansion.

Loose hop expansions can occur at one or more hops along an LSP's path. This process is referred to as loose path reoptimization.

### Tunnel Reoptimization Procedure

Tunnel reoptimization is the signaling of an LSP that is more optimal than the LSP a TE tunnel is currently using (for example, it may be shorter or may have a lower cost), and the switching over of the tunnel's data to use this new LSP.

The new more optimal TE LSP is always established and the data moved onto it before the original LSP is torn down (so it is called the “make before break” procedure). This ensures that no data packets are lost during the transition to the new LSP.

For tunnel reoptimization to function:

- Each router must be configured with the **mpls traffic-eng reoptimize events link-up** command.
- Each passive link must have an assigned administrative weight. To configure an administrative weight, use the **mpls traffic-eng administrative-weight** command in interface configuration mode.

The TE LSPs reoptimization process is triggered under the following circumstances:

- Periodically (based on a timer)
- User entered a command (**mpls traffic-eng reoptimize**) requesting reoptimization
- Network event, such as a link-up

Regardless of how reoptimization is triggered, the headend router reoptimizes a tunnel only if it can find a better path than the one the tunnel currently uses. If there is not a better path in the local topology database, no new LSP is signaled and reoptimization does not occur.

Prior to the addition of loose path reoptimization, interarea TE LSPs were not reoptimized if a better path became available in any area beyond the headend area. This is because the headend router was not capable of finding a better path when the better path existed in an area beyond its view (that is, it was not in its local topology database).

With the addition of loose path reoptimization, a tunnel's headend can reoptimize LSPs even if they span multiple areas, levels, or autonomous systems. This is done via the implementation of a query and response protocol defined in *draft-vasseur-mpls-loose-path-reopt-02.txt*. This draft defines a protocol whereby a tunnel's headend may query downstream routers to perform ERO expansion for this tunnel's LSP. These downstream routers respond in the affirmative if they can find a more optimal path than the one in use. (This is done via a new ERO expansion.) Having received an affirmative answer to its query, a headend signals a new LSP for the tunnel, and the new LSP benefits from a new ERO expansion along the better path.

Loose path reoptimization is on by default, and cannot be disabled. Whenever an LSP reoptimization is attempted but the headend fails to find a better path, if the LSP contains loose ERO subobjects, a query is sent downstream to determine whether downstream routers can find a better path. If an affirmative answer comes back, the LSP is reoptimized. That is, a new LSP is signaled (which will follow the better path), the tunnel's data packets are switched over to use this new LSP, and the original LSP is torn down.

For details on this query and response protocol, see *draft-vasseur-mpls-loose-path-reopt-02.txt*.

## ASBR Forced Link Flooding

When you configure forced link flooding on an interface, the MPLS TE link management module advertises the link to all nodes. As a result of this advertisement, the TE topology database on all the nodes within the Inter-AS is updated with this information.

ASBR forced link flooding allows the links to be advertised even if IGP adjacencies are not running over these links. TE LSPs can traverse these links at the edge of a network between two nodes running BGP (or static routes) even if the exit ASBR is not listed in the IP explicit path. Therefore, a headend LSR can consider that link when it computes its TE LSP path.

### Configuration of ASBR Forced Link Flooding

To activate ASBR forced link flooding, configure a link as passive and provide neighbor information (that is, the neighbor IGP ID and the neighbor TE ID). The required configuration tasks are described in the [“Configuring a Static Route from the MP to the PLR”](#) section on page 14.

### Link Flooding

A passive link is configured on an interface of an ASBR. The link is flooded in the ASBR's IGP. All the links are flooded as point-to-point links.

Flooding notifications are also sent when there is a change to a link's property.

### OSPF Flooding

OSPF floods opaque link-state advertisement (LSA) Type 10 link information.

If a multiaccess link has more than one neighbor, a Type 10 LSA is advertised for each neighbor. In the topology database, neighbors are represented by point-to-point neighbor relationships.

### Link TLV

A link TLV describes a single link and contains multiple sub-TLVs.

An opaque LSA contains a single link TLV.

For each ASBR-to-ASBR link, an ASBR must flood an opaque LSA containing one link TLV that has the link's attributes.

A link TLV comprises the following sub-TLVs:

- Link type (1 octet)—(Required) Defines the type of the link. The link type of a passive interface always is 1 (point-to-point), even for a multiaccess subnetwork.
- Link ID (4 octets)—(Required) Identifies the other end of the link for a point-to-point link. Includes the system ID of the neighbor, requires static configuration for a multiaccess ASBR-to-ASBR link, and includes the system ID of the neighbor.
- Local interface IP address (4 octets)—Specifies the IP addresses of the neighbor's interface corresponding to this link.
- Remote interface IP address (4 octets)—Specifies the IP addresses of the neighbor's interface corresponding to this link. The remote interface IP address is set to the router ID of the next hop. There must be a static configuration for the ASBR-to-ASBR link.
- Traffic engineering metric (4 octets)
- Maximum bandwidth (4 octets)
- Maximum reservable bandwidth (4 octets)
- Unreserved bandwidth (32 octets)
- Administrative group (4 octets)

### IS-IS TLV

In IS-IS, when autonomous system A1 floods its LSP, it includes the system ID and a pseudonode number.

If three autonomous systems are connected to a multiaccess network LAN, each link is considered to be a point-to-point link. The links are marked with the maximum metric value so that the inter-ASBR links are considered by CSPF and not by shortest path first (SPF).

TE uses the protocol TLV type 22, which has the following data structure:

- System ID and pseudonode number node (7 octets)
- Default metric (3 octets)
- Length of sub-TLVs (1 octet)
- Sub-TLVs (0 to 244 octets), where each sub-TLV consists of a sequence of the following: 1 octet for subtype, 1 octet for the length of the value field of the sub-TLV, and 0 to 242 octets for the value

Table 1 defines the sub-TLVs.

**Table 1**                      **Sub-TLVs**

| Sub-TLV | Length (Octets) | Name                                                                                                   |
|---------|-----------------|--------------------------------------------------------------------------------------------------------|
| 3       | 4               | Administrative group (color).                                                                          |
| 6       | 4               | IPv4 address for the interface described by the main TLV.                                              |
| 8       | 4               | IPv4 address for a neighboring router on this link. This will be set to the router ID of the next hop. |
| 9       | 4               | Maximum link bandwidth.                                                                                |
| 10      | 4               | Reservable link bandwidth.                                                                             |
| 11      | 32              | Unreserved bandwidth.                                                                                  |
| 18      | 3               | TE default metric.                                                                                     |



**Table 1**      **Sub-TLVs (continued)**

| Sub-TLV    | Length (Octets) | Name                                    |
|------------|-----------------|-----------------------------------------|
| 250 to 254 | —               | Reserved for Cisco-specific extensions. |
| 255        | —               | Reserved for future expansion.          |

**Note**

The TE router ID is TLV type 134.

**Topology Database**

When the topology database module receives a link-state advertisement (LSA), the module scans the LSA to find the neighbors of the links. The ASBR link is part of the same LSA and is installed in the TE topology database like any other link.

During the CSPF operation, the TE headend module uses the TE topology database to find a path to the destination. Because the Inter-AS links are part of the TE topology database, the CSPF operation uses these links to compute the LSP path.

## Link Flooding

The IGP floods information about a link in the following situations:

- When a link goes down
- When a link's configuration is changed (for example, when the link cost is modified)
- When it is time to periodically reflood the router's IGP information
- When link bandwidth changes significantly

Flooding is a little different in IS-IS and OSPF. In OSPF, only information about the link that has changed is flooded, because a Type 10 LSA contains a single link advertisement. In IS-IS, information about all links on a node is flooded even if only one has changed, because the Type 22 TLV contains a list of all links on the router.

## How to Configure MPLS Traffic Engineering: Inter-AS TE

This section contains the following procedures for configuring MPLS Traffic Engineering: Inter-AS TE:

- [Configuring Loose Hops, page 12](#)
- [Configuring a Static Route from the MP to the PLR, page 14](#)
- [Configuring ASBR Forced Link Flooding, page 15](#)

**Note**

There is no configuration procedure for loose path reoptimization.

## Configuring Loose Hops

The section describes how to do the following so that there can be loose hops:

- [Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link, page 12](#) (required)
- [Configuring a Route to Reach the Remote ASBR, page 14](#) (required)

### Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link

If you want a tunnel to span multiple networks, configure an explicit path on the tunnel that will cross the Inter-AS link by performing the following steps.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip explicit-path {name *path-name* | identifier *number*} [enable | disable]**
4. **next-address loose *A.B.C.D***
5. **interface tunnel *number***
6. **tunnel mpls traffic-eng fast-reroute**
7. **mpls traffic-eng reoptimize events link-up**

#### DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                                                                                                                       |
| Step 3 | <b>ip explicit-path {name <i>path-name</i>   identifier <i>number</i>} [enable   disable]</b><br><br><b>Example:</b><br>Router(config)# ip explicit-path identifier 2 enable | Enters the subcommand mode for IP explicit paths and creates or modifies the explicit path. This command places the router in IP explicit path configuration mode.                                                                      |
| Step 4 | <b>next-address loose <i>A.B.C.D</i></b><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# next-address loose 10.10.0.2                                                    | Specifies the next loose IP address in the explicit path. Each area border router (ABR) the path must traverse should be specified in a <b>next-address loose</b> command. This command places the router in global configuration mode. |

|        | Command or Action                                                                                                                      | Purpose                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 100                                   | Configures a tunnel interface. This command places the router in interface configuration mode.                 |
| Step 6 | <b>tunnel mpls traffic-eng fast-reroute</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng fast-reroute          | Enables an MPLS traffic engineering tunnel to use an established backup tunnel in the event of a link failure. |
| Step 7 | <b>mpls traffic-eng reoptimize events link-up</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng reoptimize events link-up | Enables automatic reoptimization of MPLS traffic engineering when an interface becomes operational.            |

## Configuring a Route to Reach the Remote ASBR

To configure a route to reach the remote ASBR, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route prefix mask {ip-address | interface-type interface-number}**

### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                               |
|--------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
|        | <b>Example:</b><br>Router> enable                                                   |                                                                                                                       |
| Step 2 | <b>configure terminal</b>                                                           | Enters global configuration mode.                                                                                     |
|        | <b>Example:</b><br>Router# configure terminal                                       |                                                                                                                       |
| Step 3 | <b>ip route prefix mask {ip-address   interface-type interface-number}</b>          | Establishes static routes.                                                                                            |
|        | <b>Example:</b><br>Router(config)# ip route 10.10.0.1<br>255.255.255.255 tunnel 101 |                                                                                                                       |

## Configuring a Static Route from the MP to the PLR

To enable Fast Reroute protection that spans across different autonomous systems, configure a static route from the MP to the PLR by performing the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route prefix mask ip-address outgoing-interface**

## DETAILED STEPS

|        | Command or Action                                                                                                                                               | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip route prefix mask ip-address outgoing-interface</b><br><br><b>Example:</b><br>Router(config)# ip route 10.10.3.1 255.255.255.255 10.0.0.0 FastEthernet0/0 | Establishes static routes.<br><br><b>Note</b> Enter this command on the MP. The destination is the PLR.          |

## Configuring ASBR Forced Link Flooding

This section describes how to do the following so that you can configure ASBR forced link flooding:

- [Configuring the Inter-AS Link as a Passive Interface Between Two ASBRs, page 15](#) (required)
- [Creating LSPs Traversing the ASBRs, page 16](#)(required)
- [Configuring Multiple Neighbors on a Link, page 18](#) (optional)

## Configuring the Inter-AS Link as a Passive Interface Between Two ASBRs

To configure the Inter-AS link as a passive interface between two ASBRs, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type slot/port**
4. **ip address ip-address mask [secondary]**
5. **mpls traffic-eng passive-interface nbr-te-id te-router-id [nbr-if-addr if-addr] [nbr-igp-id {isis sysid | ospf sysid}]**
6. **mpls traffic-eng administrative-weight weight**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                                                                                                                                                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                             |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code>                                                                                                                                                                                  | Enters global configuration mode.                                                                                                                             |
| Step 3 | <code>interface type slot/port</code><br><br><b>Example:</b><br>Router(config)# <code>interface serial 2/0</code>                                                                                                                                                                  | Specifies an interface and enters interface configuration mode.                                                                                               |
| Step 4 | <code>ip address ip-address mask [secondary]</code><br><br><b>Example:</b><br>Router(config-if)# <code>ip address 10.10.4.1 255.255.255.0</code>                                                                                                                                   | Sets a primary or secondary IP address for an interface.                                                                                                      |
| Step 5 | <code>mpls traffic-eng passive-interface nbr-te-id te-router-id [nbr-if-addr if-addr] [nbr-igp-id {isis sysid   ospf sysid}]</code><br><br><b>Example:</b><br>Router(config-if)# <code>mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id ospf 10.10.15.18</code> | Configures a link as a passive interface between two ASBRs.<br><br><b>Note</b> For an RSVP Hello configuration on the Inter-AS link, all fields are required. |
| Step 6 | <code>mpls traffic-eng administrative-weight weight</code><br><br><b>Example:</b><br>Router(config-if)# <code>mpls traffic-eng administrative-weight 20</code>                                                                                                                     | Overrides the Interior Gateway Protocol (IGP) administrative weight (cost) of the link and assigns a specific weight for the link.                            |

## Creating LSPs Traversing the ASBRs

To create LSPs traversing the ASBRs, perform the following steps.

**Note**

Perform Steps 3 through 7 for the primary LSP and then for the backup LSP.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip explicit path name enable`
4. `next-address loose A.B.C.D`
5. `interface tunnel number`

6. **tunnel mpls traffic-eng fast-reroute**
7. **tunnel mpls traffic-eng path-option** *number* { **dynamic** | **explicit** | { **name** *path-name* | *path-number* } } [**lockdown**]

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                   | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                      | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip explicit path name enable</b><br><br><b>Example:</b><br>Router(config)# ip explicit path routel enable                                                                                                                                                        | Specifies the name of the explicit path and enables the path.                                                    |
| Step 4 | <b>next-address loose A.B.C.D</b><br><br><b>Example:</b><br>Router(config)# next-address loose 10.10.10.2                                                                                                                                                           | Configures a loose hop.                                                                                          |
| Step 5 | <b>interface tunnel number</b><br><br><b>Example:</b><br>Router(config)# interface tunnel 100                                                                                                                                                                       | Configures a tunnel interface and enters interface configuration mode.                                           |
| Step 6 | <b>tunnel mpls traffic-eng fast-reroute</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng fast-reroute                                                                                                                                       | Enables an MPLS traffic engineering tunnel to use an established backup tunnel in the event of a link failure.   |
| Step 7 | <b>tunnel mpls traffic-eng path-option</b> <i>number</i> { <b>dynamic</b>   <b>explicit</b>   { <b>name</b> <i>path-name</i>   <i>path-number</i> } } [ <b>lockdown</b> ]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option 1 routel | Configures a path option for an MPLS traffic engineering tunnel.                                                 |

## Configuring Multiple Neighbors on a Link

To configure multiple neighbors on a link, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls traffic-eng passive-interface** [*nbr-te-id*] [*router-id | te-id*] [*nbr-igp-id*] [*isis sysid | ospf sysid*]
5. **mpls traffic-eng administrative-weight** *weight*

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                     | Purpose                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                        | Enters global configuration mode.                                                                                                  |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface serial 2/0                                                                                                                                                                                 | Specifies an interface and enters interface configuration mode.                                                                    |
| Step 4 | <b>mpls traffic-eng passive-interface</b> [ <i>nbr-te-id</i> ] [ <i>router-id   te-id</i> ] [ <i>nbr-igp-id</i> ] [ <i>isis sysid   ospf sysid</i> ]<br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4<br>nbr-igp-id ospf 10.10.0.4 | Configures a link as a passive link.                                                                                               |
| Step 5 | <b>mpls traffic-eng administrative-weight</b> <i>weight</i><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng administrative-weight 20                                                                                                                                    | Overrides the Interior Gateway Protocol (IGP) administrative weight (cost) of the link and assigns a specific weight for the link. |

### Troubleshooting Tips

The following debug commands are useful for troubleshooting issues with MPLS Traffic Engineering: Inter-AS TE.



**Note**

The **debug** commands are described in detail in the *Cisco IOS Debug Command Reference*, Release 12.4.

**Debugging Headend of TE LSPs**

```
debug mpls traffic-eng path lookup
debug mpls traffic-eng path verify
debug mpls traffic-eng path spf
```

**Debugging Head and Midpoint (Link-Related Debugs)**

```
debug mpls traffic-eng link-management igp-neighbors
debug mpls traffic-eng link-management advertisements
debug mpls traffic-eng link-management bandwidth-allocation
debug mpls traffic-eng link-management routing
```

## Verifying the Inter-AS TE Configuration

To verify the Inter-AS TE configuration, perform the following steps.

**Note**

Perform Step 1 for Fast Reroute ready, and Step 2 for Fast Reroute active.

### SUMMARY STEPS

1. **show ip rsvp sender detail**
2. **show ip rsvp sender detail**
3. **show mpls traffic-eng link-management advertisements**

### DETAILED STEPS

#### Step 1 **show ip rsvp sender detail**

Use this command to display the MP sender display for the primary tunnel when Fast Reroute is ready.

```
Router# show ip rsvp sender detail
```

```
PATH:
Tun Dest: 10.10.0.6 Tun ID: 100 Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1 LSP ID: 31
Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: Rl_t100
ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
  10.10.7.1/32, Flags:0x0 (No Local Protection)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
  10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
```

```
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated
```

## Step 2 show ip rsvp sender detail

Use this command to display the MP sender display when the primary tunnel is Fast Reroute active:

```
Router# show ip rsvp sender detail
```

```
PATH:
Tun Dest: 10.10.0.6 Tun ID: 100 Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1 LSP ID: 31
Path refreshes:
  arriving: from PHOP 10.10.3.1 on Et1/0 every 30000 msec
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  Session Name: R1_t100
ERO: (incoming)
  10.10.0.4 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Loose IPv4 Prefix, 8 bytes, /32)
RRO:
  10.10.3.1/32, Flags:0xB (Local Prot Avail/In Use/to NNHOP) !Ready
  10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Active
  Orig Input I/F: Et0/0
  Orig PHOP: 10.10.7.1
  Now using Bkup Filterspec w/ sender: 10.10.3.1 LSP ID: 31
  Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated
```

## Step 3 show mpls traffic-eng link-management advertisements

Use this command to display the influence of a passive link. On R2, the passive link to R4 is in the Link ID:: 1 section.

```
Router# show mpls traffic-eng link-management advertisements
```

```
Flooding Status: ready
Configured Areas: 2
IGP Area[1] ID:: ospf 1 area 0
System Information::
  Flooding Protocol: OSPF
Header Information::
  IGP System ID: 10.10.0.2
  MPLS TE Router ID: 10.10.0.2
  Flooded Links: 2
Link ID:: 1
  Link Subnet Type: Point-to-Point
  Link IP Address: 10.10.4.1
  IGP Neighbor: ID 0-0-0-0-0-0, IP 10.10.0.4
  Physical Bandwidth: 1544 kbits/sec
  Res. Global BW: 1158 kbits/sec
  Res. Sub BW: 0 kbits/sec
  Downstream::
```

```

Global Pool Sub Pool
-----
Reservable Bandwidth[0]: 1158      0 kbits/sec
Reservable Bandwidth[1]: 1158      0 kbits/sec
Reservable Bandwidth[2]: 1158      0 kbits/sec
Reservable Bandwidth[3]: 1158      0 kbits/sec
Reservable Bandwidth[4]: 1158      0 kbits/sec
Reservable Bandwidth[5]: 1158      0 kbits/sec
Reservable Bandwidth[6]: 1158      0 kbits/sec
Reservable Bandwidth[7]: 1148      0 kbits/sec
Attribute Flags: 0x00000000
IGP Area[1] ID:: ospf 1 area 1
System Information::
  Flooding Protocol: OSPF
Header Information::
  IGP System ID: 10.10.0.2
  MPLS TE Router ID: 10.10.0.2
  Flooded Links: 2
Link ID:: 1
Link Subnet Type: Point-to-Point
Link IP Address: 10.10.4.1
IGP Neighbor: ID 0-0-0-0-0-0-0, IP 10.10.0.4
Physical Bandwidth: 1544 kbits/sec
Res. Global BW: 1158 kbits/sec
Res. Sub BW: 0 kbits/sec
Downstream::

Global Pool Sub Pool
-----
Reservable Bandwidth[0]: 1158      0 kbits/sec
Reservable Bandwidth[1]: 1158      0 kbits/sec
Reservable Bandwidth[2]: 1158      0 kbits/sec
Reservable Bandwidth[3]: 1158      0 kbits/sec
Reservable Bandwidth[4]: 1158      0 kbits/sec
Reservable Bandwidth[5]: 1158      0 kbits/sec
Reservable Bandwidth[6]: 1158      0 kbits/sec
Reservable Bandwidth[7]: 1148      0 kbits/sec
Attribute Flags: 0x00000000

```

## Configuration Examples for MPLS Traffic Engineering: Inter-AS TE

This section provides the following configuration examples for MPLS Traffic Engineering: Inter-AS TE:

- [Configuring Loose Hops: Examples, page 21](#)
- [Configuring a Static Route from the MP to the PLR: Example, page 22](#)
- [Configuring ASBR Forced Link Flooding: Examples, page 22](#)

### Configuring Loose Hops: Examples

This section includes the following:

- [Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link: Example, page 22](#)
- [Configuring a Route to Reach the Remote ASBR in the IP Routing Table: Example, page 22](#)

## Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link: Example

The following commands configure a loose IP explicit path named `route1` suitable for use as a path option with Inter-AS TE with the destination 10.10.10.6 that is to traverse ABRs 10.10.0.2 and 10.10.0.4. The tunnel headend and the specified ABRs will find a path from the source AS100 to the destination 10.10.0.6 in AS200. See [Figure 1](#).

```
Router(config)# ip explicit-path name route1 enable
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4
Router(cfg-ip-expl-path)# next-address loose 10.10.0.6
```

Note that the explicit path for an interarea TE tunnel need not specify the destination router because the tunnel configuration specifies it in the tunnel destination command. The following commands configure an explicit path named `path-without-tailend` that would work equally well for the interarea tunnel created in the previous example:

```
Router(config)# ip explicit-path name path-without-tailend
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4
```

## Configuring a Route to Reach the Remote ASBR in the IP Routing Table: Example

In the following example, packets for the ASBR whose router ID is 10.10.0.1 will be forwarded via tunnel 101:

```
Router> enable
Router# configure terminal
Router(config)# ip route 10.10.0.1 255.255.255.255 tunnel 101
```

## Configuring a Static Route from the MP to the PLR: Example

In the following example, a static route is configured from the MP to the PLR. The outgoing interface is tunnel 103.

```
Router> enable
Router# configure terminal
Router(config)# ip route 10.10.3.1 255.255.255.255 tunnel 103
```

## Configuring ASBR Forced Link Flooding: Examples

This section includes the following ASBR forced link flooding examples:

- [Configuring the Inter-AS Link as a Passive Interface: Example, page 23](#)
- [Creating LSPs Traversing the ASBRs: Example, page 24](#)
- [Configuring Multiple Neighbors on a Link: Example, page 24](#)

## Configuring the Inter-AS Link as a Passive Interface: Example

For this example, see [Figure 1](#).

Routers R2 and R4 have the following router IDs:

- Router R2—10.10.0.2
- Router R4—10.10.0.4

```
Router> enable
Router# configure terminal
Router(config)# interface serial 2/0
```

### Configures OSPF on Router R2 When Its Neighbor Is Running OSPF Too

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4
```



#### Note

Because both routers are running OSPF, the **nbr-igp-id** keyword is not specified.

### Specifies That Both Router R2 and Its Neighbor Are Running OSPF (the nbr-igp-id Keyword Is Specified)

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
```

### Configures IS-IS on Router R1

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id isis 40.0000.0002.0001.00
```

### Configures the Neighbor IGP ID (nbr-igp-id) When There Is More than One Neighbor Specified on a Link

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
```

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.7 nbr-igp-id ospf 10.10.0.7
```

### Overrides the Interior Gateway Protocol (IGP) Administrative Weight of the Link and Assigns a Specific Weight

```
Router(config-if)# mpls traffic-eng administrative-weight 20
```



#### Note

The ID is unique for each neighbor.

### Configures a Link as a Passive Interface (Includes Global TE Commands)

```
interface serial 2/0
 ip address 10.10.4.1.255.255.255.0
 mpls traffic-eng tunnels
 mpls traffic-eng administrative-weight 10
 mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
 ip rsvp bandwidth 1000
 mpls traffic-eng administrative-weight 20
```

## Creating LSPs Traversing the ASBRs: Example

In the following example, a primary LSP is created:

```
Router> enable
Router# configure terminal
Router(config)# ip explicit path route1 enable
Router(config)# next-address loose 10.10.0.2
Router(config)# next-address loose 10.10.0.4
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 100
Router(config-if)# tunnel mpls traffic-eng fast reroute
Router(config-if)# tunnel mpls traffic-eng path-option 1 route1
```

In the following example, a backup LSP is created:

```
Router> enable
Router# configure terminal
Router(config)# ip explicit path backpath1 enable
Router(config)# next-address loose 10.10.0.3
Router(config)# next-address loose 10.10.0.5
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 102
Router(config)# mpls traffic-eng backup path tunnel 102
Router(config-if)# tunnel mpls traffic-eng path-option 1 backpath1
```

## Configuring Multiple Neighbors on a Link: Example

In the following example, there is more than one neighbor on a link:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/0
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf
10.10.0.4
Router(config-if)# mpls traffic-eng administrative-weight 20
```

# Additional References

The following sections provide references related to the MPLS Traffic Engineering: Inter-AS TE feature.

## Related Documents

| Related Topic                                                                                                                       | Document Title                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| MPLS traffic engineering commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                               |
| Fast Reroute                                                                                                                        | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a> |
| Link flooding and node protection                                                                                                   | <a href="#">MPLS Traffic Engineering: Interarea Tunnels</a>                                                             |
| IS-IS configuration tasks                                                                                                           | <a href="#">Configuring a Basic IS-IS Network</a>                                                                       |
| OSPF configuration tasks                                                                                                            | <a href="#">Configuring OSPF</a>                                                                                        |
| IS-IS and OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples           | <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>                                                        |
| RSVP                                                                                                                                | <a href="#">RSVP Message Authentication</a>                                                                             |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                        | Title                                                                       |
|---------------------------------------------|-----------------------------------------------------------------------------|
| RFC 3209                                    | <a href="#">Extensions to RSVP for LSP Tunnels</a>                          |
| draft-ietf-mpls-rsvp-lsp-fastreroute-02.txt | <a href="#">Fast Reroute Extensions to RSVP-TE for LSP Tunnels</a>          |
| draft-vasseur-mpls-loose-path-reopt-02.txt  | <a href="#">Reoptimization of an Explicitly Loosely Routed MPLS TE Path</a> |

| RFCs                                   | Title                                           |
|----------------------------------------|-------------------------------------------------|
| draft-vasseur-mpls-inter-as-te-00.txt  | <i>MPLS Inter-AS Traffic Engineering</i>        |
| draft-ietf-mpls-soft-preemption-00.txt | <i>MPLS Traffic Engineering Soft Preemption</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html).

For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **mpls traffic-eng passive-interface**



# Feature Information for MPLS Traffic Engineering: Inter-AS TE

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/cfn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

**Table 2** Feature Information for MPLS Traffic Engineering: Inter-AS TE

| Feature Name                          | Releases                                                            | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering: Inter-AS TE | 12.0(29)S<br>12.2(33)SRA<br>12.2(33)SRB<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS Traffic Engineering: Inter-AS TE feature provides ASBR node protection, loose path reoptimization, SSO recovery of LSPs that include loose hops, ASBR forced link flooding, Cisco IOS RSVP local policy extensions for Inter-AS, and per-neighbor key capabilities.</p> <p>In 12.0(29)S, this feature was introduced.</p> <p>In 12.2(33)SRA, the <b>nbr-if-addr</b> keyword was added to the <b>mpls traffic-eng passive-interface</b> command.</p> <p>In 12.2(33)SRB, support was added for SSO recovery of LSPs that include loose hops.</p> <p>In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>In 12.4(20)T, this feature was integrated into Cisco IOS Release 12.4(20)T.</p> |

# Glossary

**ABR**—Area Border Router. A routers connecting two areas.

**adjacency**—The MPLS TE Forwarding Adjacency feature allows a network administrator to handle a traffic engineering, label-switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm. A forwarding adjacency can be created between routers regardless of their location in the network. The routers can be located multiple hops from each other.

**area**—A logical set of network segments (for example, one that is OSPF-based) and their attached devices. Areas usually are connected to other areas by routers, making up a single autonomous system. OSPF and IS-IS define their areas differently. OSPF area borders are marked by routers. Some interfaces are in one area, and other interfaces are in another area. With IS-IS, all the routers are completely within an area, and the area borders are on links, not on routers. The routers that connect the areas are level-2 routers, and routers that have no direct connectivity to another area are level-1 routers.

**ASBR**—Autonomous System Boundary Router. The router is located between an OSPF autonomous system and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as RIP. ASBRs must reside in a nonstub OSPF area.

**autonomous system**—A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas.

**backup tunnel**—An MPLS traffic engineering tunnel used to protect other (primary) tunnel's traffic when a link or node failure occurs.

**BGP**—Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems.

**border router**—A router at the edge of a provider network that interfaces to another provider's border router using extended BGP procedures.

**Cisco Express Forwarding**—A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**Fast Reroute**—A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**flooding**—A traffic-passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

**forwarding adjacency**—A traffic engineering link (or LSP) into an IS-IS or OSPF network.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**Inter-AS LSP**—An MPLS traffic engineering label-switched path (LSP) that traverses hops that are not in the headend's topology database (that is, it is not in the same OSPF area, IS-IS area, or autonomous system as the headend).

**interface**—A network connection.

**IP explicit path**—A list of IP addresses, each representing a node or link in the explicit path.

**IS-IS**—Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where intermediate system (IS) routers exchange routing information based on a single metric to determine the network topology.

**link**—A point-to-point connection between adjacent nodes.

**LSA**—link-state advertisement. A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.

**LSP**—label-switched path. A configured connection between two routers, in which MPLS is used to carry packets. An LSP is a path created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.

**midpoint**—A transit router for a given LSP.

**midpoint reoptimization**—Ability of a midpoint to trigger a headend reoptimization.

**MP**—merge point. The LSR where one or more backup tunnels rejoin the path of the protected LSP, downstream of the potential failure. An LSR can be both an MP and a PLR simultaneously.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**multicast**—Single packets are copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination address field. (Multicast is an efficient paradigm for transmitting the same data to multiple receivers, because of its concept of a Group address. This allows a group of receivers to listen to the single address.)

**node**—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

**OSPF**—Open Shortest Path First. A link-state, hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**opaque LSA**—If a router understands LSA Type 10 link information, the router continues flooding the link throughout the network.

**passive link**—When IGP is not running on the link between two ASBRs, traffic engineering informs the IGP to flood link information on behalf of that link (that is, it advertises that link).

**PLR**—point of local repair. The headend LSR of a backup tunnel.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**RSVP**—Resource Reservation Protocol. An IETF protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

**SPF**—shortest path first. A routing algorithm used as the basis for OSPF operations. When an SPF router is powered up, it initializes its routing-protocol data structures and then waits for indications from lower-layer protocols that its interfaces are functional.

**SRLG**—Shared Risk Link Group. Sets of links that are likely to go down together (for example, because they have the same underlying fiber).

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**TLV**—type, length, values. A block of information embedded in Cisco Discovery Protocol advertisements.

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

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

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

© 2004–2008 Cisco Systems, Inc. All rights reserved.



# MPLS Traffic Engineering: Shared Risk Link Groups

---

**First Published: May 6, 2004**

**Last Updated: July 11, 2008**

The MPLS Traffic Engineering: Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same Shared Risk Link Group (SRLG) as interfaces the backup tunnel is protecting.

SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

This document contains information about and instructions for configuring the MPLS Traffic Engineering: Shared Risk Link Groups feature.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS Traffic Engineering: Shared Risk Link Groups” section on page 20](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS Traffic Engineering: Shared Risk Link Groups, page 2](#)
- [Restrictions for MPLS Traffic Engineering: Shared Risk Link Groups, page 2](#)
- [Information About MPLS Traffic Engineering: Shared Risk Link Groups, page 2](#)
- [How to Configure MPLS Traffic Engineering: Shared Risk Link Groups, page 7](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for MPLS Traffic Engineering: Shared Risk Link Groups, page 15](#)
- [Additional References, page 18](#)
- [Command Reference, page 19](#)
- [Feature Information for MPLS Traffic Engineering: Shared Risk Link Groups, page 20](#)
- [Glossary, page 22](#)

## Prerequisites for MPLS Traffic Engineering: Shared Risk Link Groups

- You must configure Fast Reroutable tunnels.
- You must enable the autotunnel backup.

## Restrictions for MPLS Traffic Engineering: Shared Risk Link Groups

- The backup tunnel must be within a single area.
- Manually created backup tunnels do not automatically avoid SRLGs of protected interfaces.
- A primary tunnel cannot be specified to avoid links belonging to specified SRLGs.

## Information About MPLS Traffic Engineering: Shared Risk Link Groups

To configure MPLS traffic engineering (MPLS TE) SRLGs, you need to understand the following concepts:

- [MPLS Traffic Engineering Brief Overview, page 2](#)
- [MPLS Traffic Engineering Shared Risk Link Groups, page 3](#)
- [Fast Reroute Protection for MPLS TE SRLGs, page 4](#)
- [Autotunnel Backup for MPLS TE SRLGs, page 5](#)

## MPLS Traffic Engineering Brief Overview

Multiprotocol Label Switching (MPLS) is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

Traffic engineering (TE) is the process of adjusting bandwidth allocations to ensure that enough is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then fixes the bandwidth available for that tunnel.

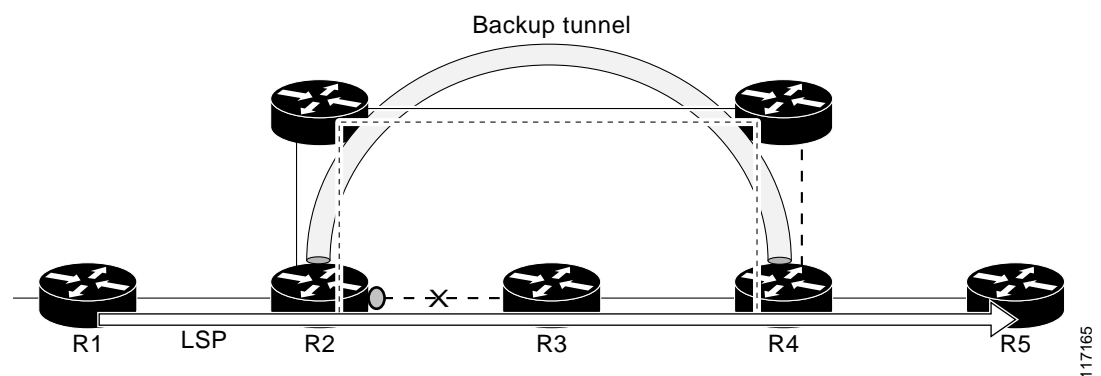
## MPLS Traffic Engineering Shared Risk Link Groups

SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

Backup tunnels should avoid using links in the same SRLG as interfaces they are protecting. Otherwise, when the protected link fails the backup tunnel fails too.

Figure 1 shows a primary label-switched path (LSP) from router R1 to router R5. The LSP protects against the failure of the R2-R3 link at R2 via a backup tunnel to R4. If the R2-R3 link fails, link protection reroutes the LSP along the backup tunnel. However, the R2-R3 link and one of the backup tunnel links are in the same SRLG. So if the R2-R3 link fails, the backup tunnel may fail too.

**Figure 1 Backup Tunnel in the Same SRLG as the Interface It Is Protecting**



The MPLS TE SRLG feature enhances backup tunnel path selection so a backup tunnel can avoid using links that are in the same SRLG as the interfaces it is protecting.

There are two ways for a backup tunnel to avoid the SRLGs of its protected interface:

- The router does not create the backup tunnel unless it avoids SRLGs of the protected interface.
- The router *tries* to avoid SRLGs of the protected interface, but if that is not possible the router creates the backup tunnel anyway. In this case there are two explicit paths. The first explicit path *tries* to avoid the SRLGs of the protected interface. If that does not work, the backup tunnel uses the second path (which ignores SRLGs).



### Note

Only backup tunnels that routers create automatically (called autotunnel backup) can avoid SRLGs of protected interfaces. For more information about these backup tunnels, see the [“Autotunnel Backup for MPLS TE SRLGs” section on page 5](#).

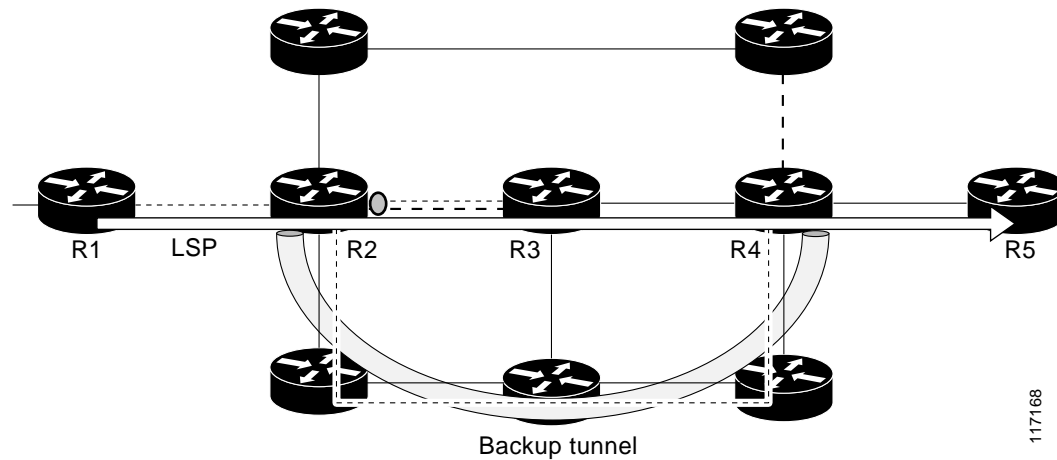
To activate the MPLS TE SRLG feature, you must do the following:

- Configure the SRLG membership of each link that has a shared risk with another link.
- Configure the routers to automatically create backup tunnels that avoid SRLGs of the protected interfaces.

For a detailed explanation of the configuration steps, see the [“How to Configure MPLS Traffic Engineering: Shared Risk Link Groups” section on page 7](#).

Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) flood the SRLG membership information (including other TE link attributes such as bandwidth availability and affinity) so that all routers in the network have the SRLG information for each link. With this topology information, routers can compute backup tunnel paths that exclude links having SRLGs in common with their protected interfaces. As shown in [Figure 2](#), the backup tunnel avoids the link between R2 and R3, which shares an SRLG with the protected interface.

**Figure 2** Backup Tunnel That Avoids SRLG of Protected Interface

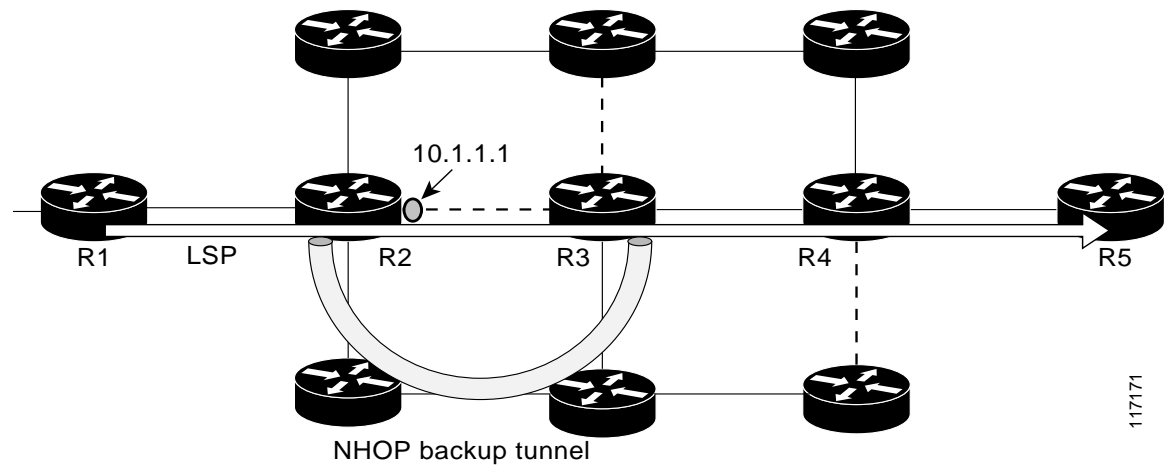


## Fast Reroute Protection for MPLS TE SRLGs

Fast Reroute (FRR) protects MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on LSPs while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

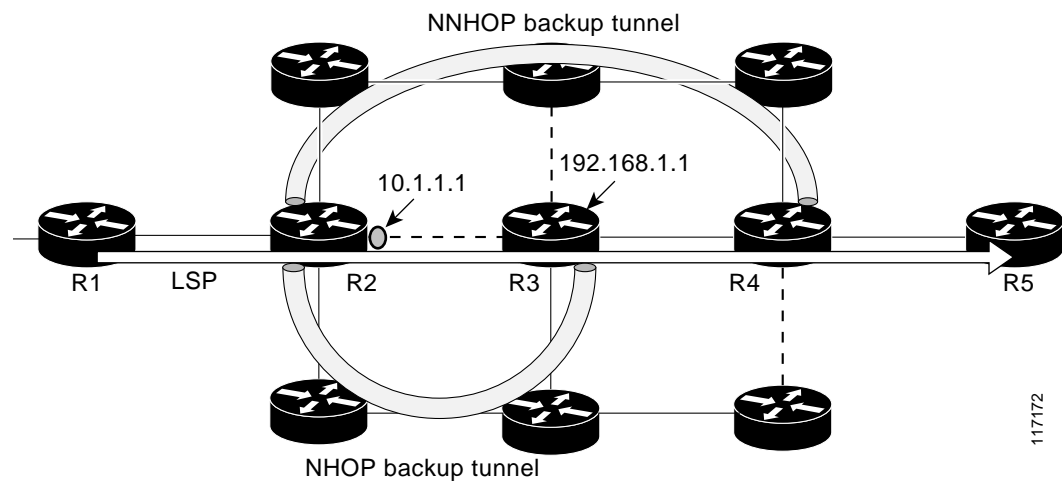
Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. [Figure 3](#) illustrates an NHOP backup tunnel.



**Figure 3** *NHOP Backup Tunnel*

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of Resource Reservation Protocol (RSVP) hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

Figure 4 illustrates an NNHOP backup tunnel.

**Figure 4** *NNHOP Backup Tunnel*

## Autotunnel Backup for MPLS TE SRLGs

Autotunnel backup is the ability of routers to create backup tunnels automatically. Therefore, you do not need to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface. Only automatically created backup tunnels can avoid SRLGs or their protected interfaces.

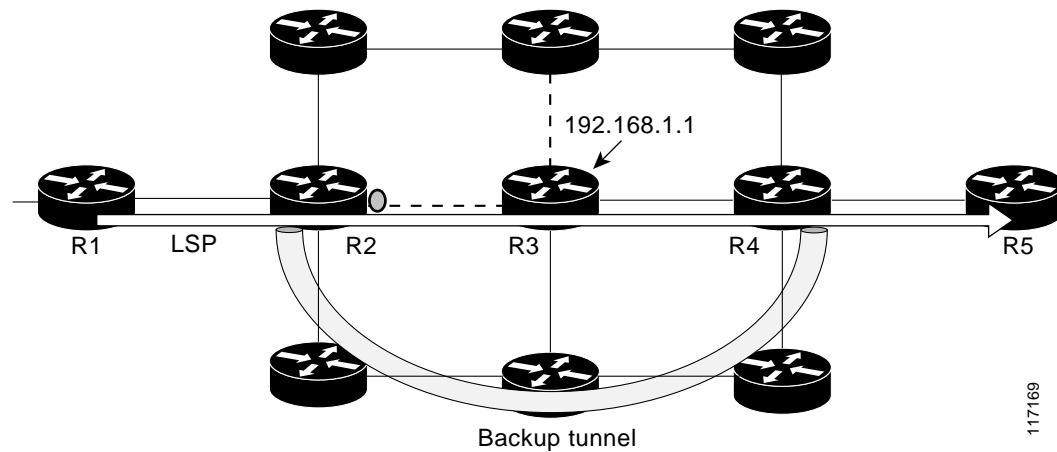
For information about backup tunnels, see the “[Fast Reroute Protection for MPLS TE SRLGs](#)” section on page 4.

For detailed information about autotunnel backup and how you can change the default command values, see [MPLS Traffic Engineering \(TE\)--AutoTunnel Primary and Backup](#).

To globally activate the autotunnel backup feature, enter the **mpls traffic-eng auto-tunnel backup** command.

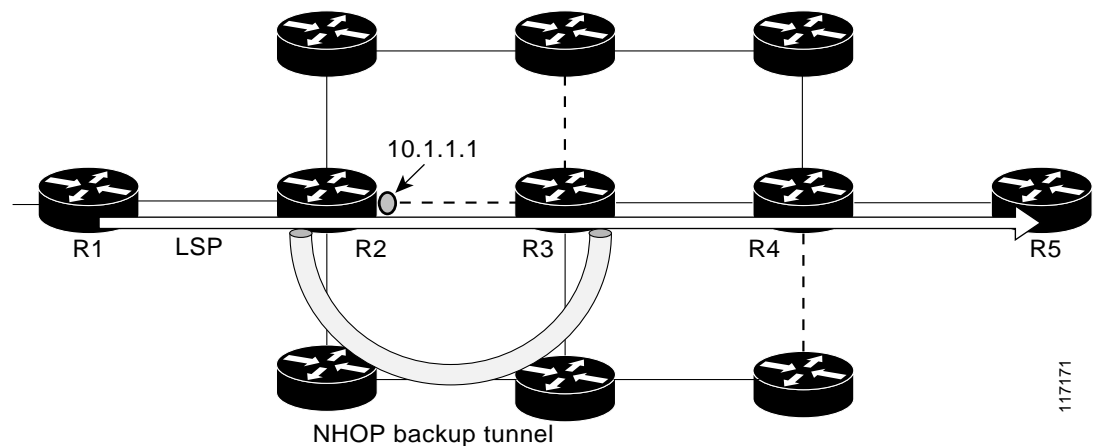
[Figure 5](#) illustrates an NNHOP automatically generated backup tunnel that excludes the router 192.168.1.1 and terminates at router R4. The backup tunnel must avoid touching any links of 192.168.1.1.

**Figure 5** Autotunnel Backup for NNHOP



[Figure 6](#) illustrates an NHOP automatically generated backup tunnel that terminates at router R3 and avoids the link 10.1.1.1, not the entire node.

**Figure 6** Autotunnel Backup for NHOP



**Note**

NNHOP excludes the router ID (the entire router must be excluded; that is, no link of the router can be included in the backup tunnel's path). NHOP excludes only the link when the backup tunnel's path is computed.

## How to Configure MPLS Traffic Engineering: Shared Risk Link Groups

This section contains the following procedures for configuring the MPLS Traffic Engineering: Shared Risk Link Groups feature:

- [Configuring MPLS TE SRLG Membership of Each Link That Has a Shared Risk with Another Link, page 7](#) (required)
- [Configuring the Routers That Automatically Create Backup Tunnels to Avoid MPLS TE SRLGs of Their Protected Interfaces, page 8](#) (required)
- [Verifying the MPLS Traffic Engineering: Shared Risk Link Groups Configuration, page 9](#) (optional)

### Configuring MPLS TE SRLG Membership of Each Link That Has a Shared Risk with Another Link

Perform the following task to configure MPLS TE SRLG membership of each link that has a shared risk with another link. Configuring SRLG membership enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same SRLG as interfaces the backup tunnel is protecting.

Enter the commands on the physical interface.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls traffic-eng srlg** [*number*]
5. **end**

#### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>interface type slot/port</pre> <p><b>Example:</b><br/>Router(config)# interface pos 1/1</p>                | <p>Specifies an interface and enters interface configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>/port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information. The slash (/) is required.</li> </ul> |
| Step 4 | <pre>mpls traffic-eng srlg [number]</pre> <p><b>Example:</b><br/>Router(config-if)# mpls traffic-eng srlg 5</p> | <p>Configures the SRLG membership of a link (interface).</p> <ul style="list-style-type: none"> <li>The <i>number</i> argument is an SRLG identifier. Valid values are 0 to 4,294,967,295.</li> </ul> <p><b>Note</b> To make the link a member of multiple SRLGs, enter the <b>mpls traffic-eng srlg</b> command multiple times.</p>                                                                                                                                                 |
| Step 5 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-if)# end</p>                                                | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring the Routers That Automatically Create Backup Tunnels to Avoid MPLS TE SRLGs of Their Protected Interfaces

Perform the following task to configure routers that automatically create backup tunnels to avoid MPLS TE SRLGs of their protected interfaces. Backup tunnels provide link protection by rerouting traffic to the next hop bypassing failed links or in this instance by avoiding SRLGs.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel backup srlg exclude [force | preferred]**
4. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>mpls traffic-eng auto-tunnel backup srlg</b><br><b>exclude [force   preferred]</b><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng auto-tunnel<br>backup srlg exclude force | Specifies that autocreated backup tunnels should avoid SRLGs of its protected interface. <ul style="list-style-type: none"> <li>The <b>force</b> keyword forces the backup tunnel to avoid SRLGs of its protected interface or interfaces.</li> <li>The <b>preferred</b> keyword causes the backup tunnel to <i>try</i> to avoid SRLGs of its protected interface or interfaces, but the backup tunnel can be created if SRLGs cannot be avoided.</li> </ul> |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Verifying the MPLS Traffic Engineering: Shared Risk Link Groups Configuration

Perform the following task to verify the MPLS traffic engineering SRLG configurations.

## SUMMARY STEPS

- enable
- show running-config
- show mpls traffic-eng link-management interfaces *interface slot/port*
- show mpls traffic-eng topology
- show mpls traffic-eng topology srlg
- show mpls traffic-eng topology brief
- show mpls traffic-eng link-management advertisements
- show ip rsvp fast-reroute
- mpls traffic-eng auto-tunnel backup srlg exclude force
- show ip explicit-paths
- show mpls traffic-eng tunnels tunnel *num*
- mpls traffic-eng auto-tunnel backup srlg exclude preferred
- show ip explicit-paths

14. **show ip rsvp fast-reroute**

15. **exit**

## DETAILED STEPS

### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password, if prompted. For example:

```
Router> enable
Router#
```

### Step 2 **show running config**

Use the following commands to configure the SRLG membership of the interface pos 3/1 and to verify that the configuration is as expected. For example:

```
Router# configure terminal
Router(config)# interface pos 3/1
Router(config-if)# mpls traffic-eng srlg 1
Router(config-if)# mpls traffic-eng srlg 2
Router(config-if)# end

Router# show running-config

interface POS 3/1
 ip address 10.0.0.33 255.255.255.255
 no ip directed-broadcast
 ip router isis
 encapsulation ppp
 no ip mroute-cache
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel5000
 mpls traffic-eng srlg 1
 mpls traffic-eng srlg 2
 tag-switching ip
 crc 32
 clock source internal
 pos ais-shut
 pos report rdool
 pos report lais
 pos report lrldi
 pos report pais
 pos report prdi
 pos report sd-ber
 isis circuit-type level-2-only
 ip rsvp bandwidth 20000 20000 sub-pool 5000
```

This verifies that the Packet over SONET (POS) interface pos 3/1 is associated that SRLG 1 and SRLG 2.

### Step 3 **show mpls traffic-eng link-management interfaces *interface slot/port***

Use this command to show the SRLG membership configured on interface pos 3/1. For example:

```
Router# show mpls traffic-eng link-management interfaces pos 3/1

System Information::
  Links Count:          11
Link ID:: PO3/1 (10.0.0.33)
  Link Status:
    SRLGs:               1 2
    Physical Bandwidth:  2488000 kbits/sec
    Max Res Global BW:   20000 kbits/sec (reserved:0% in, 0% out)
```

```

Max Res Sub BW:      5000 kbits/sec (reserved:0% in, 0% out)
MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
Inbound Admission:   allow-all
Outbound Admission:  allow-if-room
Admin. Weight:       10 (IGP)
IGP Neighbor Count:  1
IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34 (Up)
Flooding Status for each configured area [1]:
IGP Area[1]: isis level-2: flooded

```

#### Step 4 show mpls traffic-eng topology

Use this command to show the SRLG link membership flooded via the Interior Gateway Protocol (IGP). For example:

```

Router# show mpls traffic-eng topology

My_System_id:0000.0000.0003.00 (isis level-2)

Signalling error holddown:10 sec Global Link Generation 9

IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node (isis
level-2)
  link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
    frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
    TE metric:10, IGP metric:10, attribute_flags:0x0
    SRLGs:1 2
    physical_bw:2488000 (kbps), max_reservable_bw_global:20000
(kbps)
    max_reservable_bw_sub:5000 (kbps)

```

|        | Total Allocated<br>BW (kbps) | Global Pool<br>Reservable<br>BW (kbps) | Sub Pool<br>Reservable<br>BW (kbps) |
|--------|------------------------------|----------------------------------------|-------------------------------------|
|        | -----                        | -----                                  | -----                               |
| bw[0]: | 0                            | 20000                                  | 5000                                |
| bw[1]: | 0                            | 20000                                  | 5000                                |
| bw[2]: | 0                            | 20000                                  | 5000                                |
| bw[3]: | 0                            | 20000                                  | 5000                                |
| bw[4]: | 0                            | 20000                                  | 5000                                |
| bw[5]: | 0                            | 20000                                  | 5000                                |

#### Step 5 show mpls traffic-eng topology srlg

Use this command to display all the links in the network that are members of a given SRLG. For example:

```

Router# show mpls traffic-eng topology srlg

MPLS TE Id:0000.0000.0003.00 (isis level-2)
  SRLG:1
    10.0.0.33
  SRLG:2
    10.0.0.33

```

The following command shows that there are two links in SRLG 1:

```

Router# show mpls traffic-eng topology srlg

MPLS TE Id:0000.0000.0003.00 (isis level-2)
  SRLG:1
    10.0.0.33
    10.0.0.49

```

**Step 6 show mpls traffic-eng topology brief**

Use this command to display brief topology information:

```
Router# show mpls traffic-eng topology brief

My_System_id:0000.0000.0003.00 (isis level-2)

Signalling error holddown:10 sec Global Link Generation 9

IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node (isis
level-2)
  link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
    frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
    TE metric:10, IGP metric:10, attribute_flags:0x0
    SRLGs:1 2
```

**Step 7 show mpls traffic-eng link-management advertisements**

Use this command to show local link information that MPLS TE link management is currently flooding into the global TE topology. For example:

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status:      ready
Configured Areas:     1
IGP Area[1] ID:: isis level-2
System Information::
  Flooding Protocol:   ISIS
Header Information::
  IGP System ID:       0000.0000.0003.00
  MPLS TE Router ID:   10.0.3.1
  Flooded Links:       2
Link ID:: 0
  Link Subnet Type:    Point-to-Point
  Link IP Address:     10.0.0.49
  IGP Neighbor:        ID 0000.0000.0007.00, IP 10.0.0.50
  TE metric:           80000
  IGP metric:          80000
  SRLGs:               None
  Physical Bandwidth:  622000 kbits/sec
  Res. Global BW:      20000 kbits/sec
  Res. Sub BW:         5000 kbits/sec
  Downstream::

                                Global Pool  Sub Pool
                                -----
  Reservable Bandwidth[0]: 20000          5000 kbits/sec
  Reservable Bandwidth[1]: 20000          5000 kbits/sec
  Reservable Bandwidth[2]: 20000          5000 kbits/sec
  Reservable Bandwidth[3]: 20000          5000 kbits/sec
  Reservable Bandwidth[4]: 20000          5000 kbits/sec
  Reservable Bandwidth[5]: 20000          5000 kbits/sec
  Reservable Bandwidth[6]: 20000          5000 kbits/sec
  Reservable Bandwidth[7]: 20000          5000 kbits/sec
  Attribute Flags:        0x00000000
Link ID:: 1
  Link Subnet Type:    Point-to-Point
  Link IP Address:     10.0.0.33
  IGP Neighbor:        ID 0000.0000.0004.00, IP 10.0.0.34
  TE metric:           10
  IGP metric:          10
  SRLGs:               1
  Physical Bandwidth:  2488000 kbits/sec
  Res. Global BW:      20000 kbits/sec
```



```

Res. Sub BW:          5000 kbits/sec
Downstream::
                        Global Pool  Sub Pool
                        -----
Reservable Bandwidth[0]: 20000      5000 kbits/sec
Reservable Bandwidth[1]: 20000      5000 kbits/sec
Reservable Bandwidth[2]: 20000      5000 kbits/sec
Reservable Bandwidth[3]: 20000      5000 kbits/sec
Reservable Bandwidth[4]: 20000      5000 kbits/sec
Reservable Bandwidth[5]: 20000      5000 kbits/sec
Reservable Bandwidth[6]: 20000      5000 kbits/sec
Reservable Bandwidth[7]: 20000      5000 kbits/sec
Attribute Flags:      0x00000000

```

**Step 8 show ip rsvp fast-reroute**

Use this command to show that the primary tunnel is going over Pos3/1 on R3, on which SRLG 1 is configured. For example:

```
Router# show ip rsvp fast-reroute
```

| Primary Tunnel | Protect I/F | BW BPS | Type | Backup Tunnel:Label | State | Level | Type |
|----------------|-------------|--------|------|---------------------|-------|-------|------|
| R3-PRP_t0      | PO3/1       | 0:G    | None | None                | None  | None  | None |

**Step 9 mpls traffic-eng auto-tunnel backup srlg exclude force**

Use the following commands to configure autotunnel backup with the **force** keyword. For example:

```

Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
Router(config)# exit

```

**Step 10 show ip explicit-paths**

Use the following command to verify that the **force** keyword is configured with the pos3/1 link excluded from the IP explicit path. For example:

```

Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 24, status non-configured)
  1:exclude-address 10.0.0.33
  2:exclude-srlg    10.0.0.33

```

**Step 11 show mpls traffic-eng tunnels tunnel num**

Use the following command to show that autotunnel backup is configured but is down because the headend router does not have any other path to signal and it cannot use pos2/1 because it belongs in the same SRLG; that is, SRLG 1. For example:

```

Router# show mpls traffic-eng tunnels tunnel 65436

Name:R3-PRP_t65436 (Tunnel65436) Destination:
10.0.4.1
Status:
  Admin:up      Oper:down  Path:not valid  Signalling:Down
  path option 1, type explicit __dynamic_tunnel65436

Config Parameters:
  Bandwidth:0      kbps (Global)  Priority:7 7  Affinity:
0x0/0xFFFF
  Metric Type:TE (default)

```

```

AutoRoute: disabled LockDown:disabled Loadshare:0
bw-based
auto-bw:disabled

Shortest Unconstrained Path Info:
Path Weight:10 (TE)
Explicit Route:10.0.0.34 10.0.4.1
History:
Tunnel:
Time since created:5 minutes, 29 seconds
Path Option 1:
Last Error:PCALC::No path to destination, 0000.0000.0004.00

```

### Step 12 **mpls traffic-eng auto-tunnel backup srlg exclude preferred**

The following commands configure autotunnel backup with the **preferred** keyword. For example:

```

Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
Router(config)# exit

```

### Step 13 **show ip explicit-paths**

The following command shows two explicit paths. The first path avoids the SRLGs of the protected interface. The second path does not avoid the SRLGs. For example:

```

Router# show ip explicit-paths

PATH __dynamic_tunnel65436 (loose source route, path complete,
generation 30, status non-configured)
  1:exclude-address 10.0.0.33
  2:exclude-srlg    10.0.0.33
PATH __dynamic_tunnel65436_pathopt2 (loose source route, path complete,
generation 33, status non-configured)
  1:exclude-address 10.0.0.33

```

### Step 14 **show ip rsvp fast-reroute**

The following command shows that the primary tunnel is protected with autotunnel backup using the second path option (see Step 10) that does not avoid the SRLGs. For example:

```

Router# show ip rsvp fast-reroute

Primary    Protect    BW          Backup
Tunnel     I/F        BPS:Type    Tunnel:Label  State  Level  Type
-----
R3-PRP_t0  PO3/1 0:G  0:G         Tu65436:0    Ready  any-unl nhop

```

The following command shows the path options for the tunnel Tu65436:

```

Router# show mpls traffic-eng tunnels tunnel 65436

Name:R3-PRP_t65436                               (Tunnel65436) Destination:
10.0.4.1
Status:
  Admin:up          Oper:up          Path:valid          Signalling:connected

  path option 2, type explicit __dynamic_tunnel65436_pathopt2 (Basis
for Setup, path weight 80020)
  path option 1, type explicit __dynamic_tunnel65436
Config Parameters:
  Bandwidth:0          kbps (Global) Priority:7 7 Affinity:
0x0/0xFFFF
  Metric Type:TE (default)

```

```

    AutoRoute: disabled LockDown:disabled Loadshare:0
bw-based
    auto-bw:disabled
Active Path Option Parameters:
    State:explicit path option 2 is active
    BandwidthOverride:disabled LockDown:disabled Verbatim:disabled

InLabel : -
OutLabel :POS2/1, 23
RSVP Signalling Info:
    Src 10.0.3.1, Dst 10.0.4.1, Tun_Id 65436, Tun_Instance 3
RSVP Path Info:
    My Address:10.0.3.1
    Explicit Route:10.0.0.50 10.0.0.66 10.0.0.113 10.0.4.1
    Record Route: NONE
    Tspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
    Record Route: NONE
    Fspec:ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
    Path Weight:10 (TE)
    Explicit Route:10.0.0.34 10.0.4.1

```

**Step 15 exit**

Use this command to exit to user EXEC mode. For example:

```

Router# exit
Router>

```

## Configuration Examples for MPLS Traffic Engineering: Shared Risk Link Groups

This section provides the following configuration examples:

- [Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link: Example, page 15](#)
- [Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces: Example, page 16](#)

### Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link: Example

The following example shows how to specify that the SRLG membership of each link has a shared risk with another link.

As shown in [Figure 7](#) and in the following commands:

- link R2-R3 = SRLG5
- link R2-R3 = SRLG6
- link R7-R4 = SRLG5
- link R1-R2 = SRLG6

```

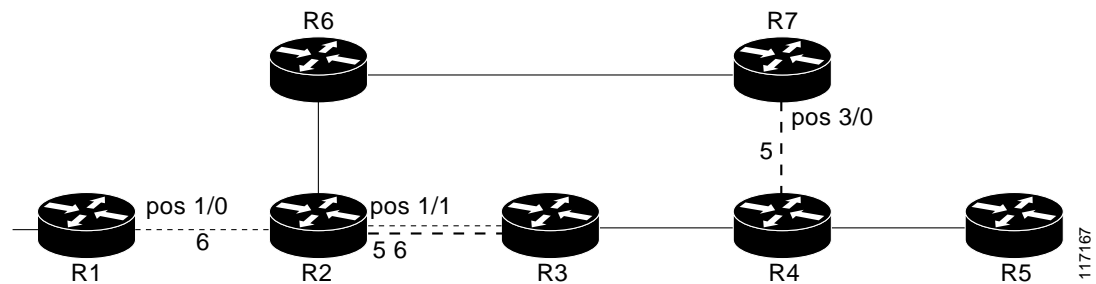
Router1# configure terminal
Router1# interface pos 1/0
Router1(config-if)# mpls traffic-eng srlg 6

Router2# configure terminal
Router2# interface pos 1/1
Router2(config-if)# mpls traffic-eng srlg 5
Router2(config-if)# mpls traffic-eng srlg 6

Router7# configure terminal
Router7# interface pos 3/0
Router7(config-if)# mpls traffic-eng srlg 5

```

**Figure 7** SRLG Membership



## Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs of Their Protected Interfaces: Example

The following example shows how to specify that automatically created backup tunnels are forced to avoid SRLGs of their protected interfaces:

```

Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force

```

[Figure 8](#) illustrates the automatically created NNHOP backup tunnel that would be created to avoid SRLGs of the protected interface if the following conditions exist:

The exclude address is 192.168.1.1.

The link at R2 has an IP address of 10.1.1.1.

The backup tunnel's explicit path avoids links that have a membership in the same SRLG as the link whose IP address is 10.1.1.1.

**Figure 8** *srlg exclude force—NNHOP Autobackup Tunnel*

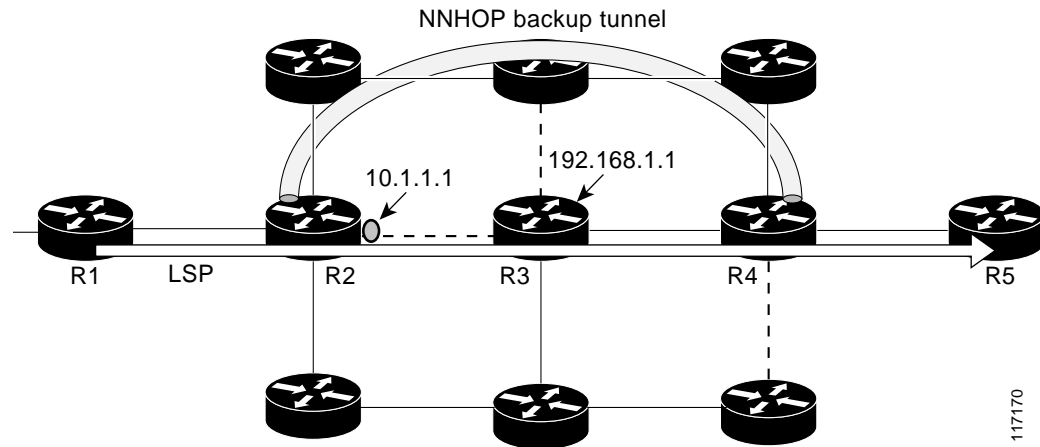
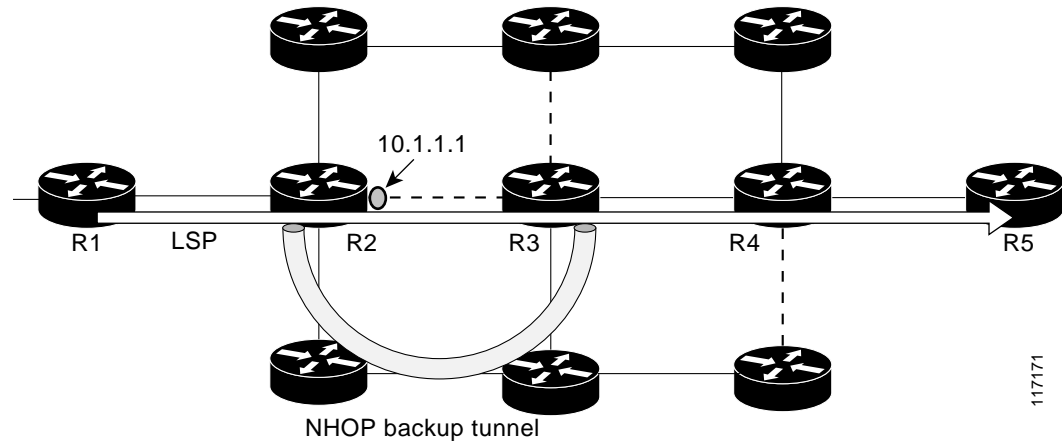


Figure 9 illustrates the automatically created NHOP backup tunnel that would be created.

**Figure 9** *srlg exclude force—NHOP Autobackup Tunnel*



## Additional References

The following sections provide references related to the MPLS Traffic Engineering: Shared Risk Link Groups feature.

### Related Documents

| Related Topic      | Document Title                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------|
| Fast Reroute       | <i>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</i> |
| IS-IS              | <i>Integrated IS-IS Routing Protocol Overview</i>                                                              |
| OSPF               | <i>Configuring OSPF</i>                                                                                        |
| Autotunnel backups | <i>MPLS Traffic Engineering AutoTunnel Primary and Backup</i>                                                  |

### Standards

| Standard | Title |
|----------|-------|
| None     | —     |

### MIBs

| MIB  | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC                                     | Title                                                  |
|-----------------------------------------|--------------------------------------------------------|
| draft-ietf-isis-gmpls-extensions-16.txt | <i>IS-IS Extensions in Support of Generalized MPLS</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **mpls traffic-eng auto-tunnel backup srlg exclude**
- **mpls traffic-eng srlg**
- **show ip explicit-paths**
- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management interfaces**
- **show mpls traffic-eng topology**

# Feature Information for MPLS Traffic Engineering: Shared Risk Link Groups

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering: Shared Risk Link Groups

| Feature Name                                      | Releases                                                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering: Shared Risk Link Groups | 12.0(28)S<br>12.0(29)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS Traffic Engineering: Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same Shared Risk Link Group (SRLG) as interfaces the backup tunnel is protecting.</p> <p>SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.</p> <p>This document contains information about and instructions for configuring the MPLS Traffic Engineering: Shared Risk Link Groups feature</p> <p>In 12.0(28)S, this feature was introduced.</p> <p>In 12.0(29)S, support was added for Open Shortest Path First (OSPF).</p> <p>In 12.2(33)SRA, this feature was integrated into a Cisco IOS 12.2SRA release</p> <p>In 12.2(33)SXH, this feature was integrated into a Cisco IOS 12.2SXH release.</p> <p>In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">MPLS Traffic Engineering Brief Overview, page 2</a></li> </ul> |



**Table 1**      *Feature Information for MPLS Traffic Engineering: Shared Risk Link Groups (continued)*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <ul style="list-style-type: none"> <li>• <a href="#">MPLS Traffic Engineering Shared Risk Link Groups, page 3</a></li> <li>• <a href="#">Fast Reroute Protection for MPLS TE SRLGs, page 4</a></li> <li>• <a href="#">Autotunnel Backup for MPLS TE SRLGs, page 5</a></li> <li>• <a href="#">Configuring MPLS TE SRLG Membership of Each Link That Has a Shared Risk with Another Link, page 7</a></li> <li>• <a href="#">Configuring the Routers That Automatically Create Backup Tunnels to Avoid MPLS TE SRLGs of Their Protected Interfaces, page 8</a></li> <li>• <a href="#">Verifying the MPLS Traffic Engineering: Shared Risk Link Groups Configuration, page 9</a></li> </ul> <p>The following commands were introduced or modified:<br/> <b>mpls traffic-eng auto-tunnel backup srlg exclude</b>, <b>mpls traffic-eng srlg</b>, <b>show ip explicit-paths</b>, <b>show mpls traffic-eng link-management advertisements</b>, <b>show mpls traffic-eng link-management interfaces</b>, and <b>show mpls traffic-eng topology</b>.</p> |

# Glossary

**Fast Reroute**—A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**IGP**—Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system.

**interface**—A network connection.

**IP address**—A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

**IP explicit path**—A list of IP addresses, each representing a node or link in the explicit path.

**IS-IS**—Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where intermediate system (IS) routers exchange routing information based on a single metric to determine the network topology.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**link**—A point-to-point connection between adjacent nodes.

**LSP**—label-switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switching router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**node**—An endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

**OSPF**—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol (IGP) routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**router ID**—Something by which a router originating a packet can be uniquely distinguished from all other routers; for example, an IP address from one of the router's interfaces.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**tunnel**—A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

© 2004–2008 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering (TE): Path Protection

---

**First Published: January 1, 2004**

**Last Updated: October 21, 2009**

The MPLS Traffic Engineering (TE): Path Protection feature provides an end-to-end failure recovery mechanism (that is, full path protection) for Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.



## Note

---

Cisco IOS Release 12.3(33)SRE and later releases support enhanced path protection, which is the ability to configure up to eight secondary path options for a given primary path option.

---

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering \(TE\): Path Protection”](#) section on [page 31](#).

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

## Contents

- [Prerequisites for MPLS Traffic Engineering \(TE\): Path Protection, page 2](#)
- [Restrictions for MPLS Traffic Engineering \(TE\): Path Protection, page 2](#)
- [Information About MPLS Traffic Engineering \(TE\): Path Protection, page 2](#)
- [How to Configure MPLS Traffic Engineering \(TE\): Path Protection, page 4](#)
- [Configuration Examples for MPLS Traffic Engineering \(TE\): Regular Path Protection, page 17](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for MPLS Traffic Engineering \(TE\): Enhanced Path Protection, page 23](#)
- [Additional References, page 29](#)
- [Feature Information for MPLS Traffic Engineering \(TE\): Path Protection, page 31](#)
- [Glossary, page 32](#)

## Prerequisites for MPLS Traffic Engineering (TE): Path Protection

- Ensure that your network supports MPLS TE, Cisco Express Forwarding, and Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).
- Enable MPLS.
- Configure TE on the routers.
- Configure a TE tunnel with a primary path option by using the **tunnel mpls traffic-eng path-option** command.
- If your router supports stateful switchover (SSO), configure Resource Reservation Protocol (RSVP) Graceful Restart in full mode on the routers.
- If your router supports SSO, for Cisco nonstop forwarding (NSF) operation you must have configured SSO on the device.

## Restrictions for MPLS Traffic Engineering (TE): Path Protection

- The secondary path will not be signaled with the FRR flag.
- Dynamic diverse paths are not supported.
- Do not use link and node protection with path protection on the headend router.
- Do not configure path protection on an automesh tunnel template because the destinations are different and you cannot use the same path option to reach multiple destinations.

## Information About MPLS Traffic Engineering (TE): Path Protection

To configure the MPLS Traffic Engineering (TE): Path Protection feature, you should understand the following concepts:

- [Traffic Engineering Tunnels, page 3](#)
- [Path Protection, page 3](#)
- [Enhanced Path Protection, page 3](#)
- [ISSU, page 4](#)
- [NSF/SSO, page 4](#)

## Traffic Engineering Tunnels

MPLS TE lets you build label switched paths (LSPs) across your network for forwarding traffic.

MPLS TE LSPs let the headend of a TE tunnel control the path its traffic takes to a particular destination. This method is more flexible than forwarding traffic based only on a destination address.

Interarea tunnels allow you to do the following:

- Build TE tunnels between areas (interarea tunnels)
- Build TE tunnels that start and end in the same area, on multiple areas on a router (intra-area tunnels)

Some tunnels are more important than others. For example, you may have tunnels carrying VoIP traffic and tunnels carrying data traffic that are competing for the same resources. MPLS TE allows you to have some tunnels preempt others. Each tunnel has a priority, and more-important tunnels take precedence over less-important tunnels.

## Path Protection

Path protection provides an end-to-end failure recovery mechanism (that is, full path protection) for MPLS TE tunnels. A secondary LSP is established, in advance, to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the headend router immediately enables the secondary LSP to temporarily carry the tunnel's traffic. If there is a failure on the secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared. Path protection can be used with a single area (OSPF or IS-IS), interarea (OSPF or IS-IS), or Inter-AS (Border Gateway Protocol (BGP), external BGP (eBGP), and static).

The failure detection mechanisms that trigger a switchover to a secondary tunnel include the following:

- Path error or resv tear from RSVP signaling
- Notification from the RSVP hello that a neighbor is lost
- Notification from the Bidirectional Forwarding Detection (BFD) protocol that a neighbor is lost
- Notification from the Interior Gateway Protocol (IGP) that the adjacency is down
- Local teardown of the protected tunnel's LSP due to preemption in order to signal higher priority LSPs, a Packet over SONET (POS) alarm, online insertion and removal (OIR), and so forth

An alternate recovery mechanism is Fast Reroute (FRR), which protects MPLS TE LSPs only from link and node failures by locally repairing the LSPs at the point of failure.

Although not as fast as link or node protection, presignaling a secondary LSP is faster than configuring a secondary primary path option or allowing the tunnel's headend router to dynamically recalculate a path. The actual recovery time is topology-dependent, and affected by delay factors such as propagation delay or switch fabric latency.

## Enhanced Path Protection

Enhanced path protection provides support of multiple backup path options per primary path option. You can configure up to eight backup path options for a given primary path option. Only one of the configured backup path options is actively signaled at any time.

After you enter the **mpls traffic-eng path-option list** command, you can enter the backup path priority in the *number* argument of the **path-option** command. A lower identifier represents a higher priority. Priorities are configurable for each backup path option. Multiple backup path options and a single backup path option cannot coexist to protect a primary path option.

## ISSU

Cisco In Service Software Upgrade (ISSU) allows you to perform a Cisco IOS software upgrade or downgrade while the system continues to forward packets. ISSU takes advantage of the Cisco IOS high availability infrastructure—Cisco nonstop forwarding (NSF) with stateful switchover (SSO) and hardware redundancy—and eliminates downtime associated with software upgrades or version changes by allowing changes while the system remains in service. Cisco ISSU lowers the impact that planned maintenance activities have on network service availability; there is less downtime and better access to critical systems.

When path protection is enabled and an ISSU upgrade is performed, path protection performance is similar to that of other TE features.

## NSF/SSO

Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure.

SSO takes advantage of Route Processor (RP) redundancy to increase network availability by establishing one of the RPs as the active processor while the other RP is designated as the secondary processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them. A switchover from the active to the secondary processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Cisco NSF works with SSO to minimize the amount of time a network is unavailable to users after a switchover. The main purpose of NSF is to continue forwarding IP packets after an RP switchover. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

The MPLS Traffic Engineering: Path Protection feature can recover after SSO. A tunnel configured for path protection may have two LSPs signaled simultaneously: the primary LSP that is carrying the traffic and the secondary LSP that carries traffic in case there is a failure along the primary path. Only information associated with one of those LSPs, the one that is currently carrying traffic, is synched to the standby RP. The standby RP, upon recovery, can determine from the checkpointed information whether the LSP was the primary or secondary.

If the primary LSP was active during the switchover, only the primary LSP is recovered. The secondary LSP that was signaled and that provided path protection is resignaled after the TE recovery period is complete. This does not impact traffic on the tunnel because the secondary LSP was not carrying traffic.

# How to Configure MPLS Traffic Engineering (TE): Path Protection

This section contains the following configuration procedures:

- [Regular Path Protection Configuration Tasks, page 5](#)



- [Enhanced Path Protection Configuration Tasks, page 10](#)

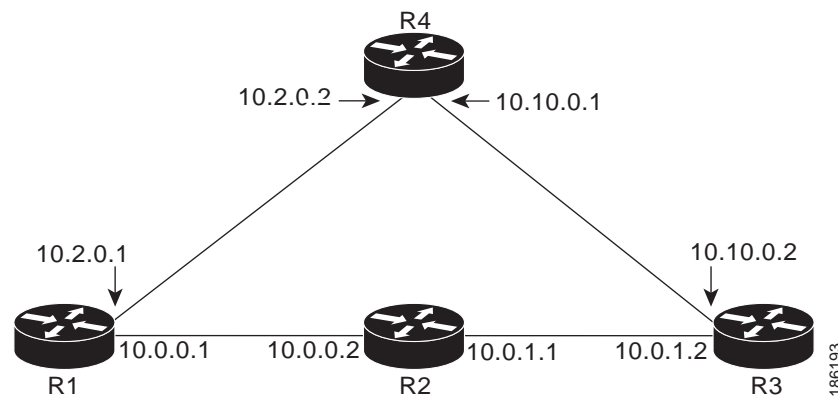
In enhanced path protection you create and assign a path option list.

## Regular Path Protection Configuration Tasks

This section contains the following tasks which are shown in [Figure 1](#).

- [Configuring Explicit Paths for Secondary Paths, page 5](#) (required)
- [Assigning a Secondary Path Option to Protect a Primary Path Option, page 6](#) (required)
- [Verifying the Configuration of MPLS Traffic Engineering Regular Path Protection, page 7](#) (optional)

**Figure 1**      **Network Topology—Path Protection**



## Configuring Explicit Paths for Secondary Paths

To specify a secondary path that does not include common links or nodes associated with the primary path in case those links or nodes go down, configure an explicit path by performing the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip explicit-path {name *path-name* | identifier *number*} [enable | disable]**
4. **index *index command* *ip-address***
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                             | Purpose                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                | Enters global configuration mode.                                                                                                                                                                   |
| Step 3 | <b>ip explicit-path</b> { <b>name</b> <i>path-name</i>   <b>identifier</b> <i>number</i> } [ <b>enable</b>   <b>disable</b> ]<br><br><b>Example:</b><br>Router(config)# ip explicit-path name path3441 enable | Creates or modifies the explicit path and enters IP explicit path configuration mode.                                                                                                               |
| Step 4 | <b>index</b> <i>index</i> <i>command</i> <i>ip-address</i><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# index 1 next-address 10.0.0.1                                                                  | Inserts or modifies a path entry at a specific index. <ul style="list-style-type: none"> <li>The IP address represents the node ID.</li> </ul> <b>Note</b> Enter this command once for each router. |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# exit                                                                                                                                          | Exits IP explicit path configuration mode and enters global configuration mode.                                                                                                                     |

## Assigning a Secondary Path Option to Protect a Primary Path Option

Assign a secondary path option in case there is a link or node failure along a path and all interfaces in your network are not protected.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel***number*
4. **tunnel mpls traffic-eng path-option protect** *number* [**attributes** *lsp-attributes* | **bandwidth** {*kpbs* | *subpool kpbs*} | **explicit** {**identifier** *path-number* | **name** *path-name*} | **list** {**name** *pathlist-name* | **identifier** *pathlist-identifier*}]

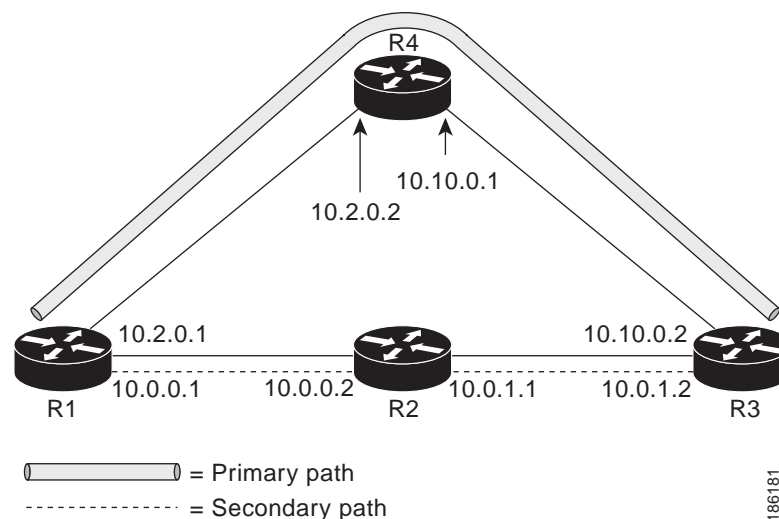
## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                                                                                                                                                                                                                                                                                                                                                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                                                                                                                                                                                                                                                                                                                              | Enters global configuration mode.                                                                                 |
| Step 3 | <code>interface tunnelnumber</code><br><br><b>Example:</b><br><code>Router(config)# interface tunnel500</code>                                                                                                                                                                                                                                                                                                                                                                 | Configures a tunnel interface and enters interface configuration mode.                                            |
| Step 4 | <code>tunnel mpls traffic-eng path-option protect</code><br><code>number [attributes lsp-attributes   bandwidth</code><br><code>{kbps   subpool kbps}   explicit {identifier</code><br><code>path-number   name path-name}   list {name</code><br><code>pathlist-name   identifier</code><br><code>pathlist-identifier}]</code><br><br><b>Example:</b><br><code>Router(config-if)# tunnel mpls traffic-eng</code><br><code>path-option protect 10 explicit name path344</code> | Configures a secondary path option for an MPLS TE tunnel.                                                         |

## Verifying the Configuration of MPLS Traffic Engineering Regular Path Protection

To verify the configuration of regular path protection, perform the following steps. In Steps 1 and 2, refer to [Figure 2](#).

**Figure 2** Network Topology Verification



## SUMMARY STEPS

1. **show running interface tunnel***tunnel-number*
2. **show mpls traffic-eng tunnels tunnel** *tunnel-interface*
3. **show mpls traffic-eng tunnels tunnel** *number* [**brief**] [**protection**]
4. **show ip rsvp high-availability database** {**hello** | **link-management** {**interfaces** | **system**} | **lsp** [**filter destination** *ip-address* / **filter lsp-id** *lsp-id* / **filter source** *ip-address* / **filter tunnel-id** *tunnel-id*] | **lsp-head** [**filter number**] | **summary**}

## DETAILED STEPS

### Step 1 **show running interface tunnel***tunnel-number*

This command shows the configuration of the primary path and protection path options.



#### Note

To show the status of both LSPs (that is, both the primary path and the protected path), use the **show mpls traffic-eng tunnels** command with the **protection** keyword.

```
Router# show running interface tunnel500

Building configuration...

Current configuration : 497 bytes
!
interface Tunnel500
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end
```

### Step 2 **show mpls traffic-eng tunnels** *tunnel-interface*

This command shows tunnel path information.

The Common Link(s) field shows the number of links shared by both the primary and secondary paths, from the headend router to the tailend router.

The Common Node(s) field shows the number of nodes shared by both the primary and secondary paths, excluding the headend and tailend routers.

As shown in the following output, there are no common links or nodes:

```
Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
```

```

Path Protection: 0 Common Link(s), 0 Common Node(s)
path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
path protect option 20, type explicit path348

```

Config Parameters:

```

Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
auto-bw: disabled

```

Active Path Option Parameters:

```

State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

```

InLabel : -

OutLabel : Ethernet1/0, 16

RSVP Signalling Info:

```

Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19

```

RSVP Path Info:

```

My Address: 10.2.0.1

```

```

Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9

```

```

Record Route: NONE

```

```

Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

```

RSVP Resv Info:

```

Record Route: NONE

```

```

Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

```

Shortest Unconstrained Path Info:

```

Path Weight: 20 (TE)

```

```

Explicit Route: 10.2.0.1 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9

```

History:

Tunnel:

```

Time since created: 11 minutes, 17 seconds

```

```

Time since path change: 8 minutes, 5 seconds

```

```

Number of LSP IDs (Tun_Instances) used: 19

```

Current LSP:

```

Uptime: 8 minutes, 5 seconds

```

### Step 3 **show mpls traffic-eng tunnels tunnel *number* [brief] [protection]**

Use this command, with the **protection** keyword specified, to show the status of both LSPs (that is, both the primary path and the protected path).



#### Note

Deleting a primary path option has the same effect as shutting down a link. Traffic will move to the protected path in use.

The following command output shows that the primary LSP is up, and the secondary LSP is up and providing protection:

```

Router# show mpls traffic-eng tunnels tunnel500 protection

```

```

R1_t500

```

```

LSP Head, Tunnel500, Admin: up, Oper: up

```

```

Src 10.1.1.1, Dest 10.0.0.9, Instance 19

```

```

Fast Reroute Protection: None

```

```

Path Protection: 0 Common Link(s), 0 Common Node(s)

```

```

Primary lsp path:10.2.0.1 10.2.0.2
                  10.10.0.1 10.10.0.2
                  10.0.0.9

```

```

Protect lsp path:10.0.0.1 10.0.0.2
                  10.0.1.1 10.0.1.2
                  10.0.0.9

```

```

Path Protect Parameters:

```

```

Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 27
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

```

The following command output shows that the primary LSP is down, and the secondary LSP is up and is actively carrying traffic:

```

Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 27
Fast Reroute Protection: None
Path Protection: Backup lsp in use.

```

**Step 4** **show ip rsvp high-availability database {hello | link-management {interfaces [fixed | variable] | system} | lsp [filter destination ip-address / filter lsp-id lsp-id / filter source ip-address / filter tunnel-id tunnel-id] | lsp-head [filter number] | summary}**

The **show ip rsvp high-availability database** command displays the contents of the RSVP high availability (HA) read and write databases used in TE. If you specify the **lsp-head** keyword, the command output includes path protection information.

```

Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
Tun ID: 500
Header:
  State: Checkpointed Action: Add
  Seq #: 3              Flags: 0x0
Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10.0.0.1
RRR path setup info
  Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
  IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
  Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
  Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
  Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
  Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
  Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0

```

## Enhanced Path Protection Configuration Tasks

This section contains the following tasks which are shown in [Figure 3](#).

- [Creating a Path Option List, page 11](#) (required)

- [Assigning a Path Option List to Protect a Primary Path Option, page 12](#) (required)
- [Verifying the Configuration of MPLS TE Enhanced Path Protection, page 13](#) (optional)

**Figure 3**      *Network Topology - Enhanced Path Protection in Cisco IOS Release 12.2(33)SRE*



## Creating a Path Option List

In Cisco IOS Release 12.2(33)SRE, perform the following task to create a path option list of backup paths for a primary path option.



### Note

To use a secondary path instead, perform the steps in the [“Configuring Explicit Paths for Secondary Paths”](#) section on page 5.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng path-option list** [**name** *pathlist-name* | **identifier** *pathlist-number*]
4. **path-option** *number* **explicit** [**name** *pathoption-name* | **identifier** *pathoption-number*]
5. **list**
6. **no** [*pathoption-name* / *pathoption-number*]
7. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                    |
| Step 3 | <b>mpls traffic-eng path-option list</b> [name pathlist-name   <b>identifier</b> pathlist-number]<br><br><b>Example:</b><br>Router(config)# mpls traffic-eng path-option list name pathlist-01       | Configures a path option list, and enters path-option list configuration mode.<br><ul style="list-style-type: none"><li>You can enter the following commands: <b>path-option</b>, <b>list</b>, <b>no</b>, and <b>exit</b>.</li></ul> |
| Step 4 | <b>path-option</b> number <b>explicit</b> [name pathoption-name   <b>identifier</b> pathoption-number]<br><br><b>Example:</b><br>Router(cfg-pathoption-list)# path-option 10 explicit identifier 200 | (Optional) Specifies the name or identification number of the path option to add, edit, or delete. The <i>pathoption-number</i> value can be from 1 through 65535.                                                                   |
| Step 5 | <b>list</b><br><br><b>Example:</b><br>Router(cfg-pathoption-list)# list                                                                                                                              | (Optional) Lists all of the path options.                                                                                                                                                                                            |
| Step 6 | <b>no</b> [pathoption-name   pathoption-number]<br><br><b>Example:</b><br>Router(cfg-pathoption-list)# no 10                                                                                         | (Optional) Deletes a specified path option.                                                                                                                                                                                          |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(cfg-pathoption-list)# exit                                                                                                                              | (Optional) Exits path-option list configuration mode and enters global configuration mode.                                                                                                                                           |

## Assigning a Path Option List to Protect a Primary Path Option

Assign a path option list in case there is a link or node failure along a path and all interfaces in your network are not protected. See [Figure 3](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**



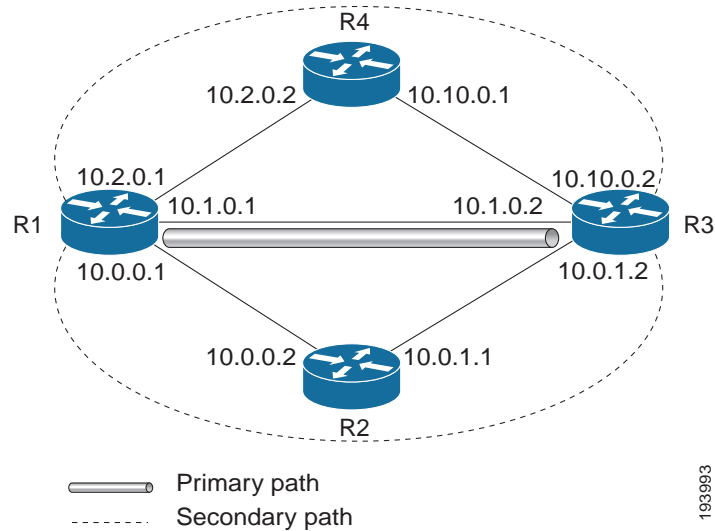
3. **interface** *tunnelnumber*
4. **tunnel mpls traffic-eng path-option protect** *number* [**attributes** *lsp-attributes* | **bandwidth** {*kbits* | *subpool kbps*} | **explicit** {**identifier** *path-number* | **name** *path-name*} | **list** {**name** *pathlist-name* | **identifier** *pathlist-identifier*}]
5. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                                                                                                                                                      | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface</b> <i>tunnelnumber</i><br><br><b>Example:</b><br>Router(config)# interface tunnel500                                                                                                                                                                                                                                                                                                                                                                                  | Configures a tunnel interface and enters interface configuration mode.                                           |
| Step 4 | <b>tunnel mpls traffic-eng path-option protect</b> <i>number</i> [ <b>attributes</b> <i>lsp-attributes</i>   <b>bandwidth</b> { <i>kbits</i>   <i>subpool kbps</i> }   <b>explicit</b> { <b>identifier</b> <i>path-number</i>   <b>name</b> <i>path-name</i> }   <b>list</b> { <b>name</b> <i>pathlist-name</i>   <b>identifier</b> <i>pathlist-identifier</i> }]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name pathlist-01 | Configures a path option list to protect primary path option 10.                                                 |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                                                                                                                                                                                                                                                                       | (Optional) Exits interface configuration mode and enters global configuration mode.                              |

## Verifying the Configuration of MPLS TE Enhanced Path Protection

To verify the configuration of MPLS TE enhanced path protection, refer to [Figure 4](#) and perform the following steps.

**Figure 4** Network Topology Verification for Enhanced Path Protection

## SUMMARY STEPS

1. `show running interface tunnel tunnel-number`
2. `show mpls traffic-eng tunnels tunnel-number`
3. `show mpls traffic-eng tunnels tunnel number [brief] [protection]`
4. `show ip rsvp high-availability database {hello | link-management {interfaces [fixed | variable] | system} | lsp [filter destination ip-address / filter lsp-id lsp-id / filter source ip-address / filter tunnel-id tunnel-id] | lsp-head [filter number] | summary}`

## DETAILED STEPS

### Step 1 `show running interface tunnel tunnel-number`

This command shows the configuration of the path option and backup path option.



#### Note

To show the status of both LSPs (that is, both the primary path and the protected path), use the `show mpls traffic-eng tunnels` command with the **protection** keyword.

```
Router# show running interface tunnel2
```

```
Building configuration..
```

```
Current configuration : 296 bytes
```

```
!
```

```
interface Tunnel2
```

```
ip unnumbered Loopback0
```

```
tunnel mode mpls traffic-eng
```

```
tunnel destination 10.10.0.2
```

```
tunnel mpls traffic-eng autoroute announce
```

```
tunnel mpls traffic-eng path-option 10 explicit name primary1
```

```
tunnel mpls traffic-eng path-option protect 10 list name pathlist-01
end
```

## Step 2 **show mpls traffic-eng tunnels tunnel *number***

This command shows tunnel path information.

The Common Link(s) field shows the number of links shared by both the primary and secondary paths, from the headend router to the tailend router.

The Common Node(s) field shows the number of nodes shared by both the primary and secondary paths, excluding the headend and tailend routers.

As shown in the following output, there are no common links or nodes:

```
Router# show mpls traffic-eng tunnels tunnel2
```

```
Name: iou-100_t2 (Tunnel2) Destination: 10.10.0.2
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
  Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 188
RSVP Path Info:
  My Address: 10.1.0.1
  Explicit Route: 10.1.0.2 10.10.0.2
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 10 (TE)
  Explicit Route: 10.1.0.1 10.1.0.2 10.10.0.2
History:
Tunnel:
  Time since created: 1 hours, 34 minutes
  Time since path change: 1 minutes, 50 seconds
  Number of LSP IDs (Tun_Instances) used: 188
Current LSP:
  Uptime: 1 minutes, 50 seconds
Prior LSP:
  ID: path option 10 [44]
  Removal Trigger: label reservation removed
```

## Step 3 **show mpls traffic-eng tunnels tunnel *number* [brief] [protection]**

Use this command, with the **protection** keyword specified, to show the status of both LSPs (that is, both the primary path and the protected path).

The following command output shows that the primary LSP is up, and the secondary LSP is up and providing protection:

```
Router# show mpls traffic-eng tunnels tunnel2 protection

iou-100_t2
LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 10.10.0.2, Instance 188
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.1.0.1 10.1.0.2
                  10.10.0.2
Protect lsp path:10.0.0.1 10.0.0.2
                  10.0.1.1 10.0.1.2
                  10.10.0.2
Path Protect Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
  Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 189
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.10.0.2
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
```

The following command output shows that the primary LSP is down, and the secondary LSP is up and is actively carrying traffic:

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 27
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
```

**Step 4** **show ip rsvp high-availability database {hello | link-management {interfaces [fixed | variable]} | system} | lsp [filter destination ip-address / filter lsp-id lsp-id / filter source ip-address / filter tunnel-id tunnel-id] | lsp-head [filter number] | summary}**

The **show ip rsvp high-availability database** command displays the contents of the RSVP HA read and write databases used in TE. If you specify the **lsp-head** keyword, the command output includes path protection information.

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
Tun ID: 2
Header:
  State: Checkpointed Action: Add
  Seq #: 2 Flags: 0x0
Data:
  lsp_id: 6, bandwidth: 0, thead_flags: 0x1, popt: 10
  feature flags: none
  output_if_num: 31, output_nhop: 10.1.0.2
RRR path setup info
  Destination: 10.10.0.2, Id: .10.10.0.2 Router Node (ospf) flag:0x0
```

```

IGP: ospf, IGP area: 0, Number of hops: 3, metric: 10
Hop 0: 10.1.0.1, Id: 10.100.100.100 Router Node (ospf), flag:0x0
Hop 1: 10.1.0.2, Id: 10.10.0.2 Router Node (ospf), flag:0x0
Hop 2: 10.103.103.103, Id: 10.10.0.2 Router Node (ospf), flag:0x0

```

## Configuration Examples for MPLS Traffic Engineering (TE): Regular Path Protection

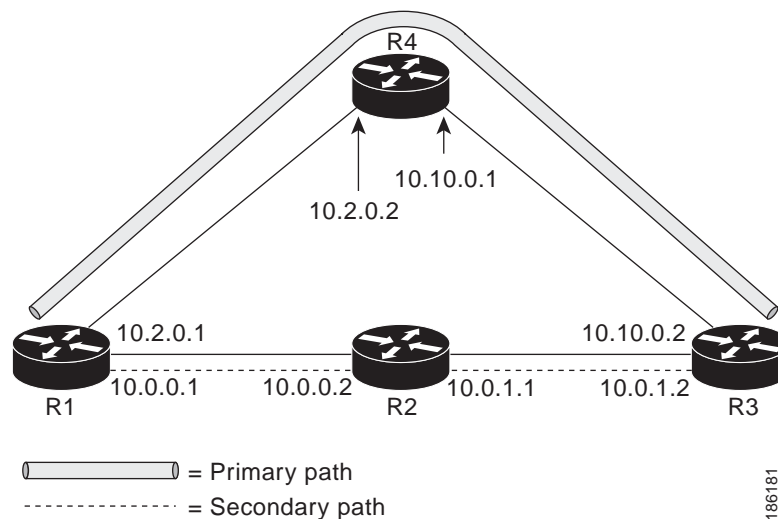
This section provides the following configuration examples for MPLS TE regular path protection:

- [Creating a Path Option List: Example, page 23](#)
- [Assigning a Path Option List to Protect a Primary Path Option: Example, page 24](#)
- [Configuring Tunnels Before and After Path Protection: Example, page 24](#)

### Configuring Explicit Paths for Secondary Paths: Example

Figure 5 illustrates a primary path and a secondary path. If there is a failure, the secondary path is used.

**Figure 5** Primary Path and Secondary Path



In the following example the explicit path is named path3441. There is an **index** command for each router. If there is failure, the secondary path is used.

```

Router(config)# ip explicit-path name path3441 enable
Router(cfg-ip-expl-path)# index 1 next 10.0.0.1
Explicit Path name path3441:
  1: next-address 10.0.0.1

Router(cfg-ip-expl-path)# index 2 next 10.0.0.2
Explicit Path name path3441:
  1: next-address 10.0.0.1

```

```

2: next-address 10.0.0.2

Router(cfg-ip-expl-path)# index 3 next 10.0.1.1
Explicit Path name path3441:
  1: next-address 10.0.0.1
  2: next-address 10.0.0.2
  3: next-address 10.0.1.1

Router(cfg-ip-expl-path)# index 4 next 10.0.1.2
Explicit Path name path3441:
  1: next-address 10.0.0.1
  2: next-address 10.0.0.2
  3: next-address 10.0.1.1
  4: next-address 10.0.1.2

Router(cfg-ip-expl-path)# exit

```

## Assigning a Secondary Path Option to Protect a Primary Path Option: Example

In the following example a traffic engineering tunnel is configured:

```

Router> enable
Router# configure terminal
Router(config-if)# interface tunnel500
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344

```

The following **show running interface** command output shows that path protection has been configured. Tunnel 500 has path option 10 using path344 and protected by path 3441, and path option 20 using path345 and protected by path348.

```

Router# show running interface tunnel500

Router# interface tunnel 500

Building configuration...

Current configuration : 497 bytes
!
interface Tunnel500
 ip unnumbered Loopback0
 tunnel destination 10.0.0.9
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 10 explicit name path344
 tunnel mpls traffic-eng path-option 20 explicit name path345
 tunnel mpls traffic-eng path-option protect 10 explicit name path3441
 tunnel mpls traffic-eng path-option protect 20 explicit name path348
end

```

## Configuring Tunnels Before and After Path Protection: Example

The **show mpls traffic-eng tunnels** command shows information about the primary (protected) path. The following sample output shows that path protection has been configured.

```

Router# show mpls traffic-eng tunnels tunnel500

```

```

Name: R1_t500    (Tunnel500)    Destination: 10.0.0.9
Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348

Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet1/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 43
RSVP Path Info:
  My Address: 10.2.0.1
  Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2
                  10.0.0.9

History:
Tunnel:
  Time since created: 18 minutes, 22 seconds
  Time since path change: 19 seconds
  Number of LSP IDs (Tun_Instances) used: 43
Current LSP:
  Uptime: 22 seconds
  Selection: reoptimization
Prior LSP:
  ID: path option 10 [27]
  Removal Trigger: reoptimization completed

```

The following **show mpls traffic-eng tunnels** command output shows information about the secondary path. Tunnel500 is protected. The protection path is used, and the primary path is down. The command output shows the IP explicit paths of the primary LSP and the secondary LSP.

```
Router# show mpls traffic-eng tunnels tunnel500 protection
```

```

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 43
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.2.0.1 10.2.0.2
                  10.10.0.1 10.10.0.2
                  10.0.0.9
Protect lsp path:10.0.0.1 10.0.0.2
                  10.0.1.1 10.0.1.2
                  10.0.0.9

```

```

Path Protect Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  InLabel : -
  OutLabel : Ethernet0/0, 17
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
  RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#

```

The following **shutdown** command shuts down the interface to use path protection:

```

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e1/0
Router(config-if)# shutdown
Router(config-if)# end
Router#

```

The following **show mpls traffic-eng tunnels** command shows that the protection path is used, and the primary path is down:

```

Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348

Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet0/0, 17
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
  RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)

```



```

Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
Tunnel:
  Time since created: 23 minutes, 28 seconds
  Time since path change: 50 seconds
  Number of LSP IDs (Tun_Instances) used: 44
Current LSP:
  Uptime: 5 minutes, 24 seconds
  Selection:
Prior LSP:
  ID: path option 10 [43]
  Removal Trigger: path error
  Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#

```

The **up** value in the Oper field of the **show mpls traffic-eng tunnels** command, with the **protection** keyword specified, shows that protection is enabled:

```

Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
  LSP Head, Tunnel500, Admin: up, Oper: up
  Src 10.1.1.1, Dest 10.0.0.9, Instance 44
  Fast Reroute Protection: None
  Path Protection: Backup lsp in use.
R1#

```

The **no shutdown** command in the following command sequence causes the interface to be up again and activates the primary path:

```

Router> enable
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface ethernet1/0
Router(config-if)# no shutdown
Router(config-if)# end

```

The following command output shows that path protection has been reestablished and the primary path is being used:

```

Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348

Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet1/0, 16

```

```

RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
RSVP Path Info:
  My Address: 10.2.0.1
  Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
  Tunnel:
    Time since created: 25 minutes, 26 seconds
    Time since path change: 23 seconds
    Number of LSP IDs (Tun_Instances) used: 52
  Current LSP:
    Uptime: 26 seconds
    Selection: reoptimization
  Prior LSP:
    ID: path option 10 [44]
    Removal Trigger: reoptimization completed
R1#

```

Following is sample **show mpls traffic-eng tunnels** command output. Tunnel500 is protected. After a failure, the primary LSP is protected.

```
Router# show mpls traffic-eng tunnels tunnel500 protection
```

```

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 52
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.2.0.1 10.2.0.2
                  10.10.0.1 10.10.0.2
                  10.0.0.9
Protect lsp path:10.0.0.1 10.0.2
                  10.0.1.1 10.0.1.2
                  10.0.0.9
Path Protect Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#

```

# Configuration Examples for MPLS Traffic Engineering (TE): Enhanced Path Protection

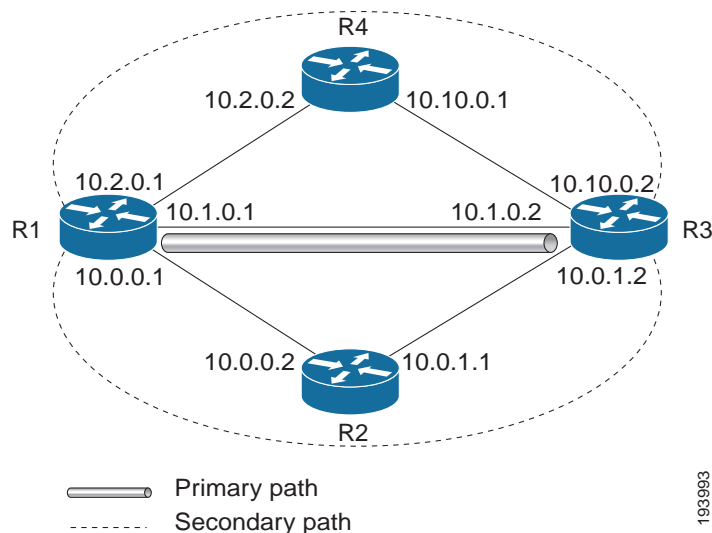
This section provides the following configuration examples for MPLS TE path protection:

- [Creating a Path Option List: Example, page 23](#)
- [Assigning a Path Option List to Protect a Primary Path Option: Example, page 24](#)
- [Configuring Tunnels Before and After Path Protection: Example, page 24](#)

## Creating a Path Option List: Example

Figure 6 shows the network topology for enhanced path protection.

**Figure 6** Network Topology for Enhanced Path Protection



The following example configures two explicit paths named **secondary1** and **secondary2**.

```
Router(config)# ip explicit-path name secondary1
Router(cfg-ip-expl-path)# index 1 next 10.0.0.2
Explicit Path name secondary1:
  1: next-address 10.0.0.2

Router(cfg-ip-expl-path)# index 2 next 10.0.1.2
Explicit Path name secondary1:
  1: next-address 10.0.0.2
  2: next-address 10.0.1.2

Router(cfg-ip-expl-path)# ip explicit-path name secondary2
Router(cfg-ip-expl-path)# index 1 next 10.2.0.2
Explicit Path name secondary2:
  1: next-address 10.2.0.2
```

```
Router(cfg-ip-expl-path)# index 2 next 10.10.0.2
Explicit Path name secondary2:
  1: next-address 10.2.0.2
  2: next-address 10.10.0.2
```

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

In the following example a path option list of backup paths is created. You define the path option list by using the explicit paths.

```
Router(config)# mpls traffic-eng path-option list name pathlist-01
Router(cfg-pathoption-list)# path-option 10 explicit name secondary1
path-option 10 explicit name secondary1
```

```
Router(cfg-pathoption-list)# path-option 20 explicit name secondary2
path-option 10 explicit name secondary1
path-option 20 explicit name secondary2
```

```
Router(cfg-pathoption-list)# exit
```

## Assigning a Path Option List to Protect a Primary Path Option: Example

In the following example, a traffic engineering tunnel is configured:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface tunnel 2
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

The following **show running interface** command output shows that path protection has been configured. Tunnel 2 has path option 10 using path primary1 and protected by secondary-list.

```
Router# show running-config interface tunnel 2

Building configuration...

Current configuration : 296 bytes
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 103.103.103.103
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name primary1
 tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

## Configuring Tunnels Before and After Path Protection: Example

The **show mpls traffic-eng tunnels** command shows information about the primary (protected) path. The following sample output shows that path protection has been configured:

```
Router# show mpls traffic-eng tunnels tunnel 2

Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
  Admin: up Oper: up Path: valid Signalling: connected
```

```

path option 10, type explicit primary1 (Basis for Setup, path weight 10)
Path Protection: 0 Common Link(s), 0 Common Node(s)
path protect option 10, type list name secondary-list
Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

```

Config Parameters:

```

Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
auto-bw: disabled

```

Active Path Option Parameters:

```

State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

```

InLabel : -

OutLabel : Ethernet7/0, implicit-null

RSVP Signalling Info:

```

Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 11

```

RSVP Path Info:

```

My Address: 10.1.0.1
Explicit Route: 10.1.0.2 103.103.103.103
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

```

RSVP Resv Info:

```

Record Route: NONE
Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

```

Shortest Unconstrained Path Info:

```

Path Weight: 10 (TE)
Explicit Route: 10.1.0.1 10.1.0.2 103.103.103.103

```

History:

Tunnel:

```

Time since created: 24 minutes, 15 seconds
Time since path change: 23 minutes, 30 seconds
Number of LSP IDs (Tun_Instances) used: 11
Current LSP:
Uptime: 23 minutes, 30 seconds

```

The following **show mpls traffic-eng tunnels** command output shows information about the secondary path. Tunnel 2 is protected.

Router# **show mpls traffic-eng tunnels tunnel 2 protection**

Router\_t2

```

LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 11
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.1.0.1 10.1.0.2
                  103.103.103.103
Protect lsp path:10.0.0.1 10.0.0.2
                  10.0.1.1 10.0.1.2
                  103.103.103.103
Path Protect Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 20
RSVP Path Info:
My Address: 10.0.0.1
Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
Record Route: NONE
Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

```

```

RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

```

The following **shutdown** command shuts down the interface to use path protection:

```

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface e7/0
Router(config-if)# shutdown
Router(config-if)# end

```

The following **show mpls traffic-eng tunnels** command shows that the protection path is used, and the primary path is down:

```

Router# show mpls traffic-eng tunnels tunnel 2

Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
  path option 10, type explicit primary1
  Path Protection: Backup lsp in use.
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: list path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 20
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103

History:
Tunnel:
  Time since created: 32 minutes, 27 seconds
  Time since path change: 1 minutes, 7 seconds
  Number of LSP IDs (Tun_Instances) used: 20
Current LSP:
  Uptime: 8 minutes, 56 seconds
Selection:
Prior LSP:
  ID: path option 10 [11]

```

```
Removal Trigger: path error
Last Error: PCALC:: No addresses to connect 100.100.100.100 to 10.1.0.2
```

The up value in the Oper field of the **show mpls traffic-eng tunnels** command, with the **protection** keyword specified, shows that protection is enabled.

```
Router# show mpls traffic-eng tunnels tunnel 2 protection
```

```
Router_t2
LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 20
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
```

The **no shutdown** command in the following command sequence causes the interface to be up again and activates the primary path:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config-if)# interface ethernet7/0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following command output shows that path protection has been reestablished and the primary path is being used:

```
Router# show mpls traffic-eng tunnels tunnel 2
```

```
Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
```

```
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
```

```
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
```

```
InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 39
RSVP Path Info:
  My Address: 10.1.0.1
  Explicit Route: 10.1.0.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 10 (TE)
  Explicit Route: 10.1.0.1 10.1.0.2 103.103.103.103
History:
  Tunnel:
  Time since created: 40 minutes, 59 seconds
```

```

Time since path change: 1 minutes, 24 seconds
Number of LSP IDs (Tun_Instances) used: 39
Current LSP:
  Uptime: 1 minutes, 27 seconds
  Selection: reoptimization
Prior LSP:
  ID: path option 10 [20]
  Removal Trigger: reoptimization completed

```

Router# **show mpls traffic-eng tunnels tunnel 2 protection**

```

Router_t2
LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 39
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.1.0.1 10.1.0.2
                  103.103.103.103
Protect lsp path:10.0.0.1 10.0.0.2
                  10.0.1.1 10.0.1.2
                  103.103.103.103
Path Protect Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet5/0, 17
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 40
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

```

The following command displays the contents of the RSVP high availability read and write databases used in TE.

Router# **show ip rsvp high-availability database lsp-head**

```

LSP_HEAD WRITE DB
Tun ID: 2
Header:
  State: Checkpointed Action: Modify
  Seq #: 17 Flags: 0x0
Data:
  lsp_id: 39, bandwidth: 0, thead_flags: 0x1, popt: 10
  feature flags: none
  output_if_num: 31, output_nhop: 10.1.0.2
RRR path setup info
  Destination: 103.103.103.103, Id: 103.103.103.103 Router Node (ospf) flag:0x0
  IGP: ospf, IGP area: 0, Number of hops: 3, metric: 10
  Hop 0: 10.1.0.1, Id: 100.100.100.100 Router Node (ospf), flag:0x0
  Hop 1: 10.1.0.2, Id: 103.103.103.103 Router Node (ospf), flag:0x0
  Hop 2: 103.103.103.103, Id: 103.103.103.103 Router Node (ospf), flag:0x0

LSP_HEAD READ DB

```



# Additional References

The following sections provide references related to the MPLS Traffic Engineering (TE): Path Protection feature.

## Related Documents

| Related Topic                     | Document Title                                                                                                                                                                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS traffic engineering commands | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                                                                         |
| RSVP                              | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>                                                                                                          |
| IS-IS                             | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li> <li>• <a href="#">Configuring a Basic IS-IS Network</a></li> </ul> |
| OSPF                              | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS IP Routing Protocols Command Reference</a></li> <li>• <a href="#">Configuring OSPF</a></li> </ul>                  |
| ISSU                              | <ul style="list-style-type: none"> <li>• <a href="#">ISSU MPLS Clients</a></li> <li>• <a href="#">ISSU and eFSU on Cisco 7600 Series Routers</a></li> </ul>                       |
| NSF/SSO                           | <a href="#">ISSU and eFSU on Cisco 7600 Series Routers</a>                                                                                                                        |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for MPLS Traffic Engineering (TE): Path Protection

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering (TE): Path Protection

| Feature Name                                   | Releases                                                             | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering (TE): Path Protection | 12.0(30)S<br>12.2(18)SXD1<br>12.2(33)SRC<br>12.4(20)T<br>12.2(33)SRE | <p>The MPLS Traffic Engineering (TE): Path Protection feature provides an end-to-end failure recovery mechanism (that is, full path protection) for MPLS TE tunnels.</p> <p>In Cisco IOS Release 12.0(30)S, this feature was introduced.</p> <p>In Cisco IOS Release 12.2(18)SXD, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SRC, support was added for In Service Software Upgrade (ISSU) and Cisco nonstop forwarding with stateful switchover (NSF/SSO). The following command was modified by this feature: <b>show ip rsvp high-availability database</b>. The following command was added: <b>tunnel mpls traffic-eng path-option protect</b>.</p> <p>In Cisco IOS Release 12.4(20)T, this feature was integrated. ISSU was not supported, and NSF with SSO was not supported. The following commands were modified: <b>show ip rsvp high-availability database</b>, <b>tunnel mpls traffic-eng path-option</b>, and <b>tunnel mpls traffic-eng path-option protect</b>.</p> <p>In Cisco IOS Release 12.2(33)SRE, support was added for enhanced path protection. The following commands were added or modified: <b>mpls traffic-eng path option list</b>, <b>show mpls traffic-eng path-option list</b>, <b>show mpls traffic-eng tunnels</b>, and <b>tunnel mpls traffic-eng path-option protect</b>.</p> |

# Glossary

**autotunnel mesh group**—An autotunnel mesh group (referred to as a mesh group) is a set of connections between edge LSRs in a network.

**backup LSP**—The LSP that is signaled to provide path protection. A backup LSP carries traffic only after failure of the primary LSP.

**backup tunnel**—An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

**BGP**—Border Gateway Protocol. An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

**Cisco Express Forwarding**—A means for accelerating the forwarding of packets within a router, by storing route lookup.

**Fast Reroute**—Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

**graceful restart**—A process for helping an RP restart after a node failure has occurred.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**interface**—A network connection.

**IS-IS**—Intermediate System-to-Intermediate System. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

**ISSU**—In Service Software Upgrade. The ISSU process allows Cisco IOS software at the router level to be updated or otherwise modified while packet forwarding continues. At the line-card level, an enhanced Fast Software Upgrade (eFSU) process minimizes line-card downtime during such upgrades to between 30 and 90 seconds by preloading the new line-card image before the ISSU switchover occurs from the active to the standby Route Processor.

**link**—A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**LSP**—label switched path. A configured connection between two routers, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**NHOP**—next hop. The next downstream node along an LSP's path.

**NHOP backup tunnel**—next-hop backup tunnel. The backup tunnel terminating at the LSP's next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

**NNHOP**—next-next hop. The node after the next downstream node along an LSP's path.

**NNHOP backup tunnel**—next-next-hop backup tunnel. The backup tunnel terminating at the LSP's next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.

**node**—The endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.

**NSF**—Cisco nonstop forwarding. Cisco NSF always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

**OSPF**—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**path option**—A path that a TE tunnel uses to reach a destination.

**path option list**—A list of backup paths as a secondary path option to protect a primary path option.

**primary LSP**—The last LSP originally signaled over the protected interface before the failure. A primary LSP is signaled by configuring a primary path option.

**primary path option**—A path that a TE tunnel uses originally to transport packets.

**primary tunnel**—A tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**protected interface**—An interface that has one or more backup tunnels associated with it.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**RP**—Route Processor. A generic term for the centralized control unit in a chassis.

**RSVP**—Resource Reservation Protocol. An IETF protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

**secondary LSP**—The LSP signaled over the protected interface before the failure. A secondary LSP is signaled by configuring a secondary path option or a path option list.

**secondary path**—A path that a TE tunnel uses to protect a primary path.

**secondary path option**—Configuration of the path option that provides protection.

**SRLG**—Shared Risk Link Group. Sets of links that are likely to go down together (for example, because they have the same underlying fiber).

**state**—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**topology**—The physical arrangement of network nodes and media within an enterprise networking structure.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**tunnel**—Secure communications path between two peers, such as two routers.

**VoIP**—Voice over IP. The capability of a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. Cisco's voice support is implemented by using voice packet technology.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# MPLS Traffic Engineering—Fast Reroute Link and Node Protection

---

**First Published:** January 16, 2003

**Last Updated:** February 27, 2009

The MPLS Traffic Engineering—Fast Reroute Link and Node Protection feature provides link protection (backup tunnels that bypass only a single link of the label-switched path (LSP)), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following Fast Reroute (FRR) features:

- Backup tunnel support
- Backup bandwidth protection
- Resource Reservation Protocol (RSVP) Hellos

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection”](#) section on page 37.

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

## Contents

- [Prerequisites for MPLS Traffic Engineering—Fast Reroute Link and Node Protection](#), page 2
- [Restrictions for MPLS Traffic Engineering—Fast Reroute Link and Node Protection](#), page 2
- [Information About MPLS Traffic Engineering—Fast Reroute Link and Node Protection](#), page 3



---

**Americas Headquarters:**

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

- [How to Configure MPLS Traffic Engineering—Fast Reroute \(FRR\) Link and Node Protection, page 17](#)
- [Configuration Examples for MPLS Traffic Engineering—Fast Reroute \(FRR\) Link and Node Protection, page 31](#)
- [Additional References, page 34](#)
- [Command Reference, page 36](#)
- [Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection, page 37](#)
- [Glossary, page 39](#)

## Prerequisites for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

Your network must support the following Cisco IOS features:

- IP Cisco Express Forwarding
- Multiprotocol Label Switching (MPLS)

Your network must support at least one of the following protocols:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

Before configuring FRR link and node protection, it is assumed that you have done the following tasks but you do not have to already have configured MPLS traffic engineering (TE) tunnels:

- Enabled MPLS TE on all relevant routers and interfaces
- Configured MPLS TE tunnels

## Restrictions for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

- Interfaces must use MPLS Global Label Allocation.
- Backup tunnel headend and tailend routers must implement FRR as described in draft-pan-rsvp-fastreroute-00.txt.
- Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.
- LSPs that are actively using backup tunnels are not considered for promotion. If an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.
- You cannot enable FRR Hellos on a router that also has Resource Reservation Protocol (RSVP) Graceful Restart enabled.



- (Applicable only to Release 12.2.) You cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with stateful switchover (SSO) redundancy. This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered by any midpoint router along the LSP's path if the router experiences an SSO switchover.
- MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.

## Information About MPLS Traffic Engineering—Fast Reroute Link and Node Protection

To configure MPLS Traffic Engineering—Fast Reroute Link and Node Protection, you need to understand the following concepts:

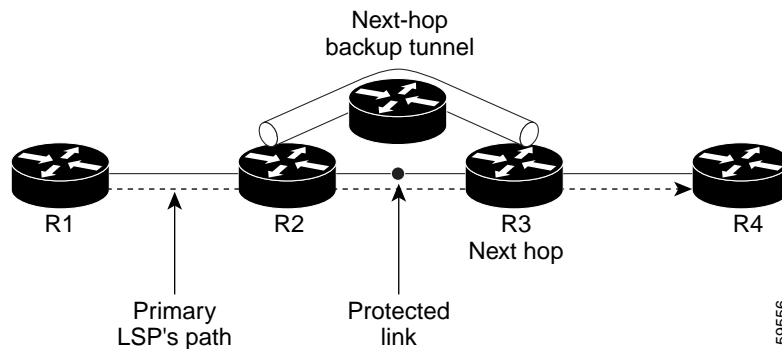
- [Fast Reroute, page 3](#)
- [Link Protection, page 3](#)
- [Node Protection, page 4](#)
- [Bandwidth Protection, page 5](#)
- [RSVP Hello, page 5](#)
- [Features of MPLS Traffic Engineering—Fast Reroute Link and Node Protection, page 6](#)
- [Fast Reroute Operation, page 8](#)

### Fast Reroute

Fast Reroute (FRR) is a mechanism for protecting MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or node.

### Link Protection

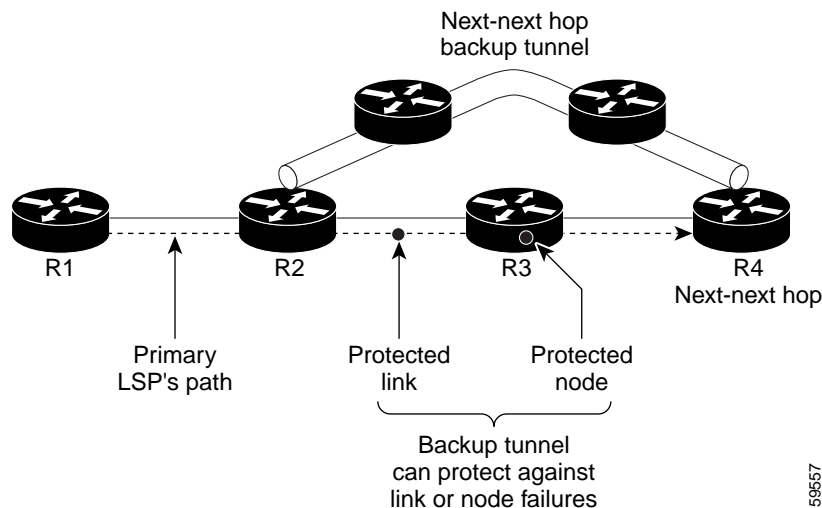
Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. [Figure 1](#) illustrates an NHOP backup tunnel.

**Figure 1** *NHOP Backup Tunnel*

## Node Protection

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

Figure 2 illustrates an NNHOP backup tunnel.

**Figure 2** *NNHOP Backup Tunnel*

If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes are the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.

- Primary LSP is modified so that FRR is disabled. (The **no mpls traffic-eng fast-reroute** command is entered.)

## Bandwidth Protection

NHOP and NNNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected. For information about mapping tunnels and assigning backup bandwidth, see the [“Backup Tunnel Selection Procedure”](#) section on page 10.

LSPs that have the “bandwidth protection desired” bit set have a higher right to select backup tunnels that provide bandwidth protection; that is, those LSPs can preempt other LSPs that do not have that bit set. For more information, see the [“Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection”](#) section on page 8.

## RSVP Hello

### RSVP Hello Operation

RSVP Hello enables RSVP nodes to detect when a neighboring node is not reachable. This provides node-to-node failure detection. When such a failure is detected, it is handled in a similar manner as a link-layer communication failure.

RSVP Hello can be used by FRR when notification of link-layer failures is not available (for example, with Ethernet), or when the failure detection mechanisms provided by the link layer are not sufficient for the timely detection of node failures.

A node running Hello sends a Hello Request to a neighboring node every interval. If the receiving node is running Hello, it responds with Hello Ack. If four intervals pass and the sending node has not received an Ack or it receives a bad message, the sending node declares that the neighbor is down and notifies FRR.

There are two configurable parameters:

- Hello interval—Use the **ip rsdp signalling hello refresh interval** command.
- Number of acknowledgment messages that are missed before the sending node declares that the neighbor is down—Use the **ip rsdp signalling hello refresh misses** command

### Hello Instance

A Hello instance implements RSVP Hello for a given router interface IP address and remote IP address. A large number of Hello requests are sent; this puts a strain on the router resources. Therefore, create a Hello instance only when it is necessary and delete it when it is no longer needed.

There are two types of Hello instances:

- [Active Hello Instances](#)

- [Passive Hello Instances](#)

#### Active Hello Instances

If a neighbor is unreachable when an LSP is ready to be fast rerouted, an active Hello instance is needed. Create an active Hello instance for each neighbor with at least one LSP in this state.

Active Hello instances periodically send Hello Request messages, and expect Hello Ack messages in response. If the expected Ack message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (lost). LSPs traversing that neighbor may be fast rerouted.

If there is a Hello instance with no LSPs for an unreachable neighbor, do not delete the Hello instance. Convert the active Hello instance to a passive Hello instance because there may be an active instance on the neighboring router that is sending Hello requests to this instance.

#### Passive Hello Instances

Passive Hello instances respond to Hello Request messages (sending Ack messages), but do not initiate Hello Request messages and do not cause LSPs to be fast rerouted. A router with multiple interfaces can run multiple Hello instances to different neighbors or to the same neighbor.

A passive Hello instance is created when a Hello Request is received from a neighbor with a source IP address/destination IP address pair in the IP header for which a Hello instance does not exist.

Delete passive instances if no Hello messages are received for this instance within 10 minutes.

## Features of MPLS Traffic Engineering—Fast Reroute Link and Node Protection

MPLS Traffic Engineering—Fast Reroute Link and Node Protection has the following features:

- [Backup Tunnel Support, page 6](#)
- [Backup Bandwidth Protection, page 7](#)
- [RSVP Hello, page 8](#)

### Backup Tunnel Support

Backup tunnel support has the following capabilities:

- [Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR, page 6](#)
- [Multiple Backup Tunnels Can Protect the Same Interface, page 6](#)
- [Backup Tunnels Provide Scalability, page 7](#)

#### Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR

Backup tunnels that terminate at the next-next hop protect both the downstream link and node. This provides protection for link and node failures. For more detailed information, see the [“Node Protection” section on page 4](#).

#### Multiple Backup Tunnels Can Protect the Same Interface

There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for node protection requires supporting multiple backup tunnels per protected interface. These backup tunnels can terminate at the same destination or at different destinations. That is, for a given protected interface, you can configure multiple NHOP or NNHOP backup tunnels. This allows redundancy and load balancing.

In addition to being required for node protection, the protection of an interface by multiple backup tunnels provides the following benefits:

- **Redundancy**—If one backup tunnel is down, other backup tunnels protect LSPs.
- **Increased backup capacity**—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels). For a more detailed explanation, see the [“Backup Tunnel Selection Procedure” section on page 10](#).

Examples are shown in the [“Backup Tunnels Terminating at Different Destinations” section on page 9](#) and the [“Backup Tunnels Terminating at the Same Destination” section on page 9](#).

### Backup Tunnels Provide Scalability

A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. An example of N:1 protection is when one backup tunnel protects 5000 LSPs, each router along the backup path maintains one additional tunnel.

One-to-one protection is when a separate backup tunnel must be used for each LSP needing protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection. An example of 1:1 protection is when 5000 backup tunnels protect 5000 LSPs, each router along the backup path must maintain state for an additional 5000 tunnels.

## Backup Bandwidth Protection

Backup bandwidth protection allows you to give LSPs carrying certain kinds of data (such as voice) priority for using backup tunnels. Backup bandwidth protection has the following capabilities:

- [Bandwidth Protection on Backup Tunnels, page 7](#)
- [Bandwidth Pool Specifications for Backup Tunnels, page 7](#)
- [Semidynamic Backup Tunnel Paths, page 7](#)
- [Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection, page 8](#)

### Bandwidth Protection on Backup Tunnels

Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.

### Bandwidth Pool Specifications for Backup Tunnels

You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using subpool bandwidth can use them or only LSPs that use global-pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could not provide bandwidth protection.

### Semidynamic Backup Tunnel Paths

The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature that was added in Release 12.0(14)ST. If you use this feature, semidynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semidynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.

### Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection

In case there are not enough NHOP or NNHOP backup tunnels or they do not have enough backup bandwidth to protect all LSPs, you can give an LSP priority in obtaining backup tunnels with bandwidth protection. This is especially useful if you want to give LSPs carrying voice a higher priority than those carrying data.

To activate this feature, enter the **tunnel mpls traffic-eng fast-reroute bw-protect** command to set the “bandwidth protection desired” bit. See the [“Enabling Fast Reroute on LSPs” section on page 17](#).

The LSPs do not necessarily *receive* bandwidth protection. They have a higher *chance* of receiving bandwidth protection if they need it.

LSPs that do not have the bandwidth protection bit set can be demoted. Demotion is when one or more LSPs are removed from their assigned backup tunnel to provide backup to an LSP that has its bandwidth protection bit set. Demotion occurs only when there is a scarcity of backup bandwidth.

When an LSP is demoted, it becomes unprotected (that is, it no longer has a backup tunnel). During the next periodic promotion cycle, an attempt is made to find the best possible backup tunnels for all LSPs that do not currently have protection, including the LSP that was demoted. The LSP may get protection at the same level or a lower level, or it may get no protection.

For information about how routers determine which LSPs to demote, see the [“Backup Protection Preemption Algorithms” section on page 14](#).

## RSVP Hello

RSVP Hello enables a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational. This feature is useful when next-hop node failure is not detectable by link layer mechanisms, or when notification of link-layer failures is not available (for example, Gigabit Ethernet). This allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

For a more detailed description of RSVP Hello, see the [“RSVP Hello” section on page 5](#).

## Fast Reroute Operation

This section describes the following:

- [Fast Reroute Activation, page 8](#)
- [Backup Tunnels Terminating at Different Destinations, page 9](#)
- [Backup Tunnels Terminating at the Same Destination, page 9](#)
- [Backup Tunnel Selection Procedure, page 10](#)
- [Bandwidth Protection, page 11](#)
- [Load Balancing on Limited-Bandwidth Backup Tunnels, page 11](#)
- [Load Balancing on Unlimited-Bandwidth Backup Tunnels, page 12](#)
- [Pool Type and Backup Tunnels, page 12](#)
- [Tunnel Selection Priorities, page 12](#)
- [Bandwidth Protection Considerations, page 14](#)

## Fast Reroute Activation

Two mechanisms cause routers to switch LSPs onto their backup tunnels:

- Interface down notification
- RSVP Hello neighbor down notification

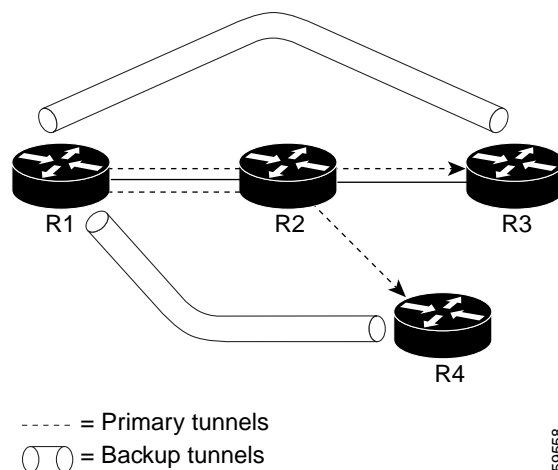
When a router's link or neighboring node fails, the router often detects this failure by an interface down notification. On a GSR Packet over SONET (PoS) interface, this notification is very fast. When a router notices that an interface has gone down, it switches LSPs going out that interface onto their respective backup tunnels (if any).

RSVP Hellos can also be used to trigger FRR. If RSVP Hellos are configured on an interface, messages are periodically sent to the neighboring router. If no response is received, Hellos declare that the neighbor is down. This causes any LSPs going out that interface to be switched to their respective backup tunnels.

## Backup Tunnels Terminating at Different Destinations

Figure 3 illustrates an interface that has multiple backup tunnels terminating at different destinations and demonstrates why, in many topologies, support for node protection requires supporting multiple backup tunnels per protected interface.

**Figure 3** Backup Tunnels That Terminate at Different Destinations



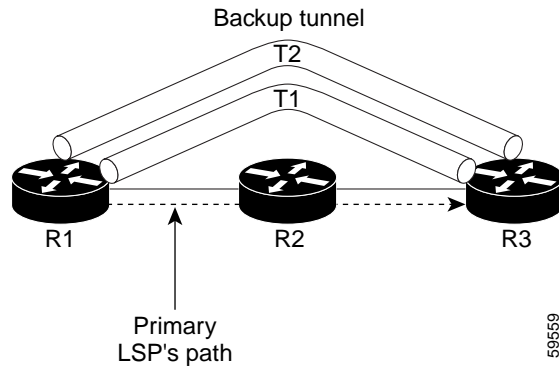
In this illustration, a single interface on R1 requires multiple backup tunnels. LSPs traverse the following routes:

- R1, R2, R3
- R1, R2, R4

To provide protection if node R2 fails, two NNHOP backup tunnels are required: one terminating at R3 and one terminating at R4.

## Backup Tunnels Terminating at the Same Destination

Figure 4 shows how backup tunnels terminating at the same location can be used for redundancy and load balancing. Redundancy and load balancing work for both NHOP and NNHOP backup tunnels.

**Figure 4 Backup Tunnels That Terminate at the Same Destination**

In this illustration, there are three routers: R1, R2, and R3. At R1 two NNHOP backup tunnels (T1 and T2) go from R1 to R3 without traversing R2.

**Redundancy**—If R2 fails or the link from R1 to R2 fails, either backup tunnel can be used. If one backup tunnel is down, the other can be used. LSPs are assigned to backup tunnels when the LSPs are first established. This is done before a failure.

**Load balancing**—If neither backup tunnel has enough bandwidth to back up all LSPs, both tunnels can be used. Some LSPs will use one backup tunnel, other LSPs will use the other backup tunnel. The router decides the best way to fit the LSPs onto the backup tunnels.

## Backup Tunnel Selection Procedure

When an LSP is signaled, each node along the LSP path that provides FRR protection for the LSP selects a backup tunnel for the LSP to use if either of the following events occurs:

- The link to the next hop fails.
- The next hop fails.

By having the node select the backup tunnel for an LSP before a failure occurs, the LSP can be rerouted onto the backup tunnel quickly if there is a failure.

For an LSP to be mapped to a backup tunnel, all of the following conditions must exist:

- The LSP is protected by FRR; that is, the LSP is configured with the **tunnel mpls traffic-eng fast-reroute** command.
- The backup tunnel is up.
- The backup tunnel is configured to have an IP address, typically a loopback address.
- The backup tunnel is configured to protect this LSP's outgoing interface; that is, the interface is configured with the **mpls traffic-eng backup-path** command.
- The backup tunnel does not traverse the LSP's protected interface.
- The backup tunnel terminates at the LSP's NHOP or NNHOP. If it is an NNHOP tunnel, it does not traverse the LSP's NHOP.
- The bandwidth protection requirements and constraints, if any, for the LSP and backup tunnel are met. For information about bandwidth protection considerations, see the [“Bandwidth Protection” section on page 11](#).



## Bandwidth Protection

A backup tunnel can be configured to protect two types of backup bandwidth:

- **Limited backup bandwidth**—A backup tunnel provides bandwidth protection. The sum of the bandwidth of all LSPs using this backup tunnel cannot exceed the backup tunnel's backup bandwidth. When you assign LSPs to this type of backup tunnel, sufficient backup bandwidth must exist.
- **Unlimited backup bandwidth**—The backup tunnel does not provide any bandwidth protection (that is, best-effort protection exists). There is no limit to the amount of bandwidth used by the LSPs that are mapped to this backup tunnel. LSPs that allocate zero bandwidth can use only backup tunnels that have unlimited backup bandwidth.

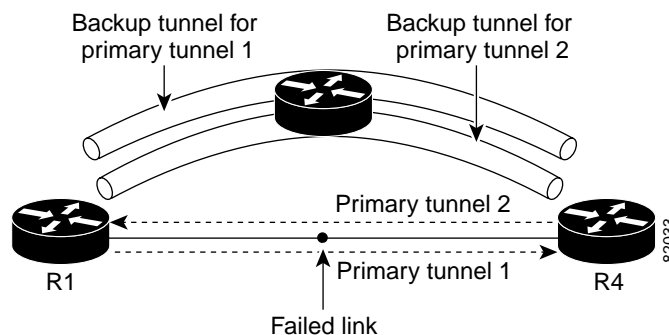
## Load Balancing on Limited-Bandwidth Backup Tunnels

There may be more than one backup tunnel that has sufficient backup bandwidth to protect a given LSP. In this case, the router chooses the one that has the least amount of backup bandwidth available. This algorithm limits fragmentation, maintaining the largest amount of backup bandwidth available.

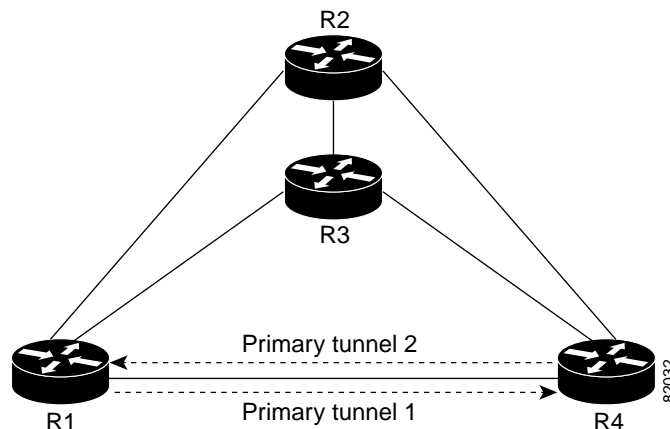
Specifying limited backup bandwidth does not “guarantee” bandwidth protection if there is a link or node failure. For example, the set of NHOP and NNHOP backup tunnels that gets triggered when an interface fails may all share some link on the network topology, and this link may not have sufficient bandwidth to support all LSPs using this set of backup tunnels.

In [Figure 5](#), both backup tunnels traverse the same links and hop. When the link between routers R1 and R4 fails, backup tunnels for primary tunnel 1 and primary tunnel 2 are triggered simultaneously. The two backup tunnels may share a link in the network.

**Figure 5** Backup Tunnels Share a Link



In [Figure 6](#), the backup tunnel for primary tunnel 1 may traverse routers R1-R2-R3-R4, and the backup tunnel for primary tunnel 2 may traverse routers R4-R2-R3-R1. In this case, the link R2-R3 may get overloaded if R1-R4 fails.

**Figure 6**      **Overloaded Link**

## Load Balancing on Unlimited-Bandwidth Backup Tunnels

More than one backup tunnel, each having unlimited backup bandwidth, can protect a given interface. In this case, when choosing a backup tunnel for a given LSP, the router chooses the backup tunnel that has the least amount of backup bandwidth in use. This algorithm evenly distributes the LSPs across backup tunnels based on an LSP's bandwidth. If an LSP is requesting zero bandwidth, the router chooses the backup tunnel that is protecting the fewest LSPs.

## Pool Type and Backup Tunnels

By default, a backup tunnel provides protection for LSPs that allocate from any pool (that is, global or subpool). However, a backup tunnel can be configured to protect only LSPs that use global-pool bandwidth, or only those that use subpool bandwidth.

## Tunnel Selection Priorities

This section describes the following:

- [NHOP Versus NNHOP Backup Tunnels](#), page 12
- [Promotion](#), page 14
- [Backup Protection Preemption Algorithms](#), page 14

### NHOP Versus NNHOP Backup Tunnels

More than one backup tunnel can protect a given LSP, where one backup tunnel terminates at the LSP's NNHOP, and the other terminates at the LSP's NHOP. In this case, the router chooses the backup tunnel that terminates at the NNHOP (that is, FRR prefers NNHOP over NHOP backup tunnels).

[Table 1](#) lists the tunnel selection priorities. The first choice is an NNHOP backup tunnel that acquires its bandwidth from a subpool or global pool, and has limited bandwidth. If there is no such backup tunnel, the next choice (2) is a next-next hop backup tunnel that acquires a limited amount of bandwidth from any pool. The preferences go from 1 (best) to 8 (worst), where choice 3 is for an NNHOP backup tunnel with an unlimited amount of subpool or global-pool bandwidth.

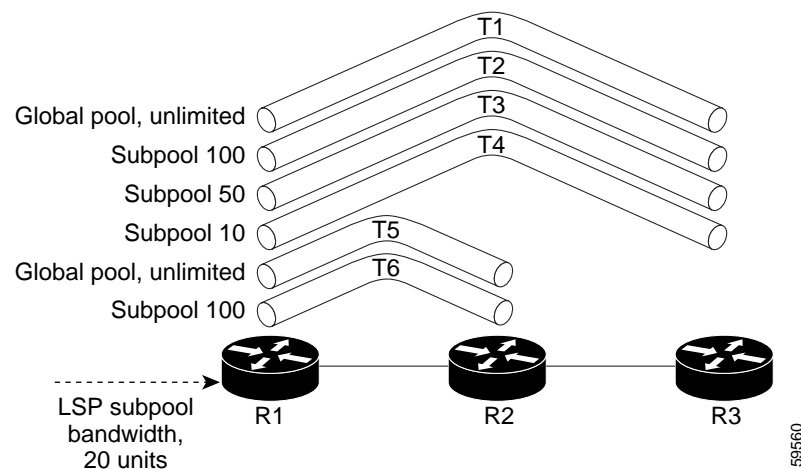
**Table 1** Tunnel Selection Priorities

| Preference | Backup Tunnel Destination | Bandwidth Pool         | Bandwidth Amount |
|------------|---------------------------|------------------------|------------------|
| 1 (Best)   | NNHOP                     | Subpool or global pool | Limited          |
| 2          | NNHOP                     | Any                    | Limited          |
| 3          | NNHOP                     | Subpool or global pool | Unlimited        |
| 4          | NNHOP                     | Any                    | Unlimited        |
| 5          | NHOP                      | Subpool or global pool | Limited          |
| 6          | NHOP                      | Any                    | Limited          |
| 7          | NHOP                      | Subpool or global pool | Unlimited        |
| 8 (Worst)  | NHOP                      | Any                    | Unlimited        |

Figure 7 shows an example of the backup tunnel selection procedure based on the designated amount of global pool and subpool bandwidth currently available.

**Note**

If NHOP and NNHOP backup tunnels do not have sufficient backup bandwidth, no consideration is given to the type of data that the LSP is carrying. For example, a voice LSP may not be protected unless it is signaled before a data LSP. To prioritize backup tunnel usage, see the “[Backup Protection Preemption Algorithms](#)” section on page 14.

**Figure 7** Choosing from Among Multiple Backup Tunnels

In this example, an LSP requires 20 units (kilobits per second) of sub-pool backup bandwidth. The best backup tunnel is selected as follows:

1. Backup tunnels T1 through T4 are considered first because they terminate at the NNHOP.
2. Tunnel T4 is eliminated because it has only ten units of sub-pool backup bandwidth.
3. Tunnel T1 is eliminated because it protects only LSPs using global-pool bandwidth.

4. Tunnel T3 is chosen over T2 because, although both have sufficient backup bandwidth, T3 has the least backup bandwidth available (leaving the most backup bandwidth available on T2).
5. Tunnels T5 and T6 need not be considered because they terminate at an NHOP, and therefore are less desirable than T3, which terminates at an NNHOP.

### Promotion

After a backup tunnel has been chosen for an LSP, conditions may change that will cause us to reevaluate this choice. This reevaluation, if successful, is called promotion. Such conditions may include:

1. A new backup tunnel comes up.
2. The currently chosen backup tunnel for this LSP goes down.
3. A backup tunnel's available backup bandwidth increases. For example, an LSP protected by the tunnel has been reoptimized by the headend to use another path.

For cases 1 and 2, the LSP's backup tunnel is evaluated immediately. Case 3 is addressed by periodically reevaluating LSP-to-backup tunnel mappings. By default, background reevaluation is performed every 5 minutes. This interval is configurable via the **mpls traffic-eng fast-reroute timers** command.

### Backup Protection Preemption Algorithms

When you set the “bandwidth protection desired” bit for an LSP, the LSP has a higher right to select backup tunnels that provide bandwidth protection and it can preempt other LSPs that do not have that bit set.

If there is insufficient backup bandwidth on NNHOP backup tunnels but not on NHOP backup tunnels, the bandwidth-protected LSP does not preempt NNHOP LSPs; it uses NHOP protection.

If there are multiple LSPs using a given backup tunnel and one or more must be demoted to provide bandwidth, there are two user-configurable methods (algorithms) that the router can use to determine which LSPs are demoted:

- Minimize amount of bandwidth that is wasted.
- Minimize the number of LSPs that are demoted.

For example, If you need ten units of backup bandwidth on a backup tunnel, you can demote one of the following:

- A single LSP using 100 units of bandwidth—Makes available more bandwidth than needed, but results in lots of waste
- Ten LSPs, each using one unit of bandwidth—Results in no wasted bandwidth, but affects more LSPs

The default algorithm is to minimize the number of LSPs that are demoted. To change the algorithm to minimize the amount of bandwidth that is wasted, enter the **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw** command.

## Bandwidth Protection Considerations

There are numerous ways in which bandwidth protection can be ensured. [Table 2](#) describes the advantages and disadvantages of three methods.

**Table 2**      **Bandwidth Protection Methods**

| Method                                                    | Advantages                                                                                                                            | Disadvantages                                                                                                                                                                             |
|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Reserve bandwidth for backup tunnels explicitly.          | It is simple.                                                                                                                         | It is a challenge to allow bandwidth sharing of backup tunnels protecting against independent failures.                                                                                   |
| Use backup tunnels that are signaled with zero bandwidth. | It provides a way to share bandwidth used for protection against independent failures, so it ensures more economical bandwidth usage. | It may be complicated to determine the proper placement of zero bandwidth tunnels.                                                                                                        |
| Backup bandwidth protection.                              | It ensures bandwidth protection for voice traffic.                                                                                    | An LSP that does not have backup bandwidth protection can be demoted at any time if there is not enough backup bandwidth and an LSP that has backup bandwidth protection needs bandwidth. |

Cisco implementation of FRR does not mandate a particular approach, and it provides the flexibility to use any of the above approaches. However, given a range of configuration choices, be sure that the choices are constant with a particular bandwidth protection strategy.

The following sections describe some important issues in choosing an appropriate configuration:

- [Using Backup Tunnels with Explicitly Signaled Bandwidth, page 15](#)
- [Using Backup Tunnels Signaled with Zero Bandwidth, page 16](#)

### Using Backup Tunnels with Explicitly Signaled Bandwidth

Two bandwidth parameters must be set for a backup tunnel:

- Actual signaled bandwidth
- Backup bandwidth

To signal bandwidth requirements of a backup tunnel, configure the bandwidth of the backup tunnel by using the **tunnel mpls traffic-eng bandwidth** command.

To configure the backup bandwidth of the backup tunnel, use the **tunnel mpls traffic-eng backup-bw** command.

The signaled bandwidth is used by the LSRs on the path of the backup tunnel to perform admission control and do appropriate bandwidth accounting.

The backup bandwidth is used by the point of local repair (PLR) (that is, the headend of the backup tunnel) to decide how much primary traffic can be rerouted to this backup tunnel if there is a failure.

Both parameters need to be set to ensure proper operation. The numerical value of the signaled bandwidth and the backup bandwidth should be the same.

### Protected Bandwidth Pools and the Bandwidth Pool from Which the Backup Tunnel Reserves Its Bandwidth

The **tunnel mpls traffic-eng bandwidth** command allows you to configure the following:

- Amount of bandwidth a backup tunnel reserves

- The DS-TE bandwidth pool from which the bandwidth needs to be reserved

**Note**

Only one pool can be selected (that is, the backup tunnel can explicitly reserve bandwidth from either the global pool or the subpool, but not both).

The **tunnel mpls traffic-eng backup-bw** command allows you to specify the bandwidth pool to which the traffic must belong for the traffic to use this backup tunnel. Multiple pools are allowed.

There is no direct correspondence between the bandwidth pool that is protected and the bandwidth pool from which the bandwidth of the backup tunnel draws its bandwidth.

Bandwidth protection for 10 Kbps of subpool traffic on a given link can be achieved by configuring any of the following command combinations:

- **tunnel mpls traffic-eng bandwidth sub-pool 10**  
**tunnel mpls traffic-eng backup-bw sub-pool 10**
- **tunnel mpls traffic-eng bandwidth global-pool 10**  
**tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool unlimited**
- **tunnel mpls traffic-eng bandwidth global-pool 40**  
**tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool 30**

**Using Backup Tunnels Signaled with Zero Bandwidth**

Frequently it is desirable to use backup tunnels with zero signaled bandwidth, even when bandwidth protection is required. It may seem that if no bandwidth is explicitly reserved, no bandwidth guarantees can be provided. However, that is not necessarily true.

In the following situation:

- Only link protection is desired.
- Bandwidth protection is desired only for sub-pool traffic.

For each protected link AB with a maximum reservable subpool value of  $n$ , there may be a path from node A to node B such that the difference between the maximum reservable global and the maximum reservable subpool is at least the value of  $n$ . If it is possible to find such paths for each link in the network, you can establish all the backup tunnels along such paths without any bandwidth reservations. If there is a single link failure, only one backup tunnel will use any link on its path. Because that path has at least  $n$  available bandwidth (in the global pool), assuming that marking and scheduling is configured to classify the subpool traffic into a priority queue, the subpool bandwidth is guaranteed.

This approach allows sharing of the global pool bandwidth between backup tunnels protecting independent link failures. The backup tunnels are expected to be used for only a short period of time after a failure (until the headends of affected LSPs reroute those LSPs to other paths with available subpool bandwidth). The probability of multiple unrelated link failures is very small (in the absence of node or shared risk link group (SRLG) failures, which result in multiple link failures). Therefore, it is reasonable to assume that link failures are in practice independent with high probability. This “independent failure assumption” in combination with backup tunnels signaled without explicit bandwidth reservation enables efficient bandwidth sharing that yields substantial bandwidth savings.

Backup tunnels protecting the subpool traffic do now draw bandwidth from any pool. Primary traffic using the global pool can use the entire global pool, and primary traffic using the subpool can use the entire subpool. Yet, subpool traffic has a complete bandwidth guarantee if there is a single link failure.

A similar approach can be used for node and SRLG protection. However, the decision of where to put the backup tunnels is more complicated because both node and SRLG failures effectively result in the simultaneous failure of several links. Therefore, the backup tunnels protecting traffic traversing all affected links cannot be computed independently of each other. The backup tunnels protecting groups of links corresponding to different failures can still be computed independently of each other, which results in similar bandwidth savings.

#### Signaled Bandwidth Versus Backup Bandwidth

Backup bandwidth is used locally (by the router that is the headend of the backup tunnel) to determine which, and how many, primary LSPs can be rerouted on a particular backup tunnel. The router ensures that the combined bandwidth requirement of these LSPs does not exceed the backup bandwidth.

Therefore, even when the backup tunnel is signaled with zero bandwidth, the backup bandwidth must be configured with the value corresponding to the actual bandwidth requirement of the traffic protected by this backup tunnel. Unlike the case when bandwidth requirements of the backup tunnels are explicitly signaled, the value of the signaled bandwidth (which is zero) is not the same value as the backup bandwidth.

## How to Configure MPLS Traffic Engineering—Fast Reroute (FRR) Link and Node Protection

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured.

This section contains the following procedures:

- [Enabling Fast Reroute on LSPs](#) (required)
- [Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop](#) (required)
- [Assigning Backup Tunnels to a Protected Interface](#) (required)
- [Associating Backup Bandwidth and Pool Type with a Backup Tunnel](#) (optional)
- [Configuring Backup Bandwidth Protection](#) (optional)
- [Configuring an Interface for Fast Link and Node Failure Detection](#) (optional)
- [Verifying That Fast Reroute Is Operational](#) (optional)

### Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if they have been configured as fast reroutable. To do this, enter the following commands at the headend of each LSP.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **tunnel mpls traffic-eng fast-reroute [bw-protect]**

## DETAILED STEPS

|        | Command                                                                                                                                               | Purpose                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                        | Enters global configuration mode.                                                                                 |
| Step 3 | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 1000                                                 | Enters interface configuration mode for the specified tunnel.                                                     |
| Step 4 | <b>tunnel mpls traffic-eng fast-reroute [bw-protect]</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect | Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure.                 |

## Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop

Creating a backup tunnel is basically no different from creating any other tunnel. To create a backup tunnel to the next hop or to the next-next hop, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the [“Finding Feature Information” section on page 1](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **ip unnumbered *interface-type interface-number***
5. **tunnel destination *ip-address***
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng path-option [protect] *number* {dynamic | explicit | {name *path-name* | *path-number*}}** [lockdown]
8. **ip explicit-path name *word***
9. **exclude-address *ip-address***



## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                              | Enters global configuration mode.                                                                                                                                                                  |
| Step 3 | <b>interface tunnel <i>number</i></b><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                                                                                                                                                                          | Creates a new tunnel interface and enters interface configuration mode.                                                                                                                            |
| Step 4 | <b>ip unnumbered <i>interface-type interface-number</i></b><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 0                                                                                                                                                           | Gives the tunnel interface an IP address that is the same as that of interface Loopback0.<br><br><b>Note</b> This command is not effective until Loopback0 has been configured with an IP address. |
| Step 5 | <b>tunnel destination <i>ip-address</i></b><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.3.3.3                                                                                                                                                                        | Specifies the IP address of the device where the tunnel will terminate. This address should be the router ID of the device that is the NHOP or NNHOP of LSPs to be protected.                      |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                                                                                                                                               | Sets the encapsulation mode of the tunnel to MPLS TE.                                                                                                                                              |
| Step 7 | <b>tunnel mpls traffic-eng path-option [<i>protect</i>] <i>preference-number</i> {dynamic   explicit   {name <i>path-name</i>   <i>path-number</i>}}[<i>lockdown</i>]</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link | Configures a path option for an MPLS TE tunnel.<br>Enters router configuration mode.                                                                                                               |

|        | Command                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <code>ip explicit-path name word</code><br><br><b>Example:</b><br>Router(config-router)# ip explicit-path name avoid-protected-link | Enters the command mode for IP explicit paths and creates the specified path. Enters explicit path command mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 9 | <code>exclude-address ip-address</code><br><br><b>Example:</b><br>Router(config-ip-expl-path)# exclude-address 3.3.3.3              | <p>For link protection, specify the IP address of the link to be protected. For node protection, specify the router ID of the node to be protected.</p> <p><b>Note</b> Backup tunnel paths can be dynamic or explicit and they do not have to use <code>exclude-address</code>. Because backup tunnels must avoid the protected link or node, it is convenient to use the <b>exclude-address</b> command.</p> <p><b>Note</b> When using the <b>exclude-address</b> command to specify the path for a backup tunnel, you must exclude an interface IP address to avoid a link (for creating an NHOP backup tunnel), or a router ID address to avoid a node (for creating an NNHOP backup tunnel).</p> |

## Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the “[Finding Feature Information](#)” section on page 1.



### Note

You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls traffic-eng backup-path tunnel** *interface*

## DETAILED STEPS

|        | Command                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface POS 5/0                                             | Moves configuration to the physical interface level, directing subsequent configuration commands to the specific physical interface identified by the <i>type</i> value. The <i>slot</i> and <i>port</i> identify the slot and port being configured. The interface must be a supported interface. See the <a href="#">“Finding Feature Information” section on page 1</a> . Enters interface configuration mode. |
| Step 4 | <b>mpls traffic-eng backup-path tunnel</b> <i>interface</i><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng backup-path tunnel 2 | Allows LSPs going out this interface to use this backup tunnel if there is a link or node failure.<br><br><b>Note</b> You can enter this command multiple times to associate multiple backup tunnels with the same protected interface.                                                                                                                                                                           |

## Associating Backup Bandwidth and Pool Type with a Backup Tunnel

To associate backup bandwidth with a backup tunnel and designate the type of LSP that can use a backup tunnel, enter the following commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *tunnel number*
4. **tunnel mpls traffic-eng backup-bw** {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}]}

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                      | Purpose                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                               | Enters global configuration mode.                                                                                                         |
| Step 3 | <b>interface tunnel number</b><br><br><b>Example:</b><br>Router(config)# interface tunnel 2                                                                                                                                  | Enters interface configuration mode for the specified tunnel.                                                                             |
| Step 4 | <b>tunnel mpls traffic-eng backup-bw {bandwidth   [sub-pool {bandwidth   Unlimited}] [global-pool {bandwidth   Unlimited}]}</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000 | Associates bandwidth with a backup tunnel and designates whether LSPs that allocate bandwidth from the specified pool can use the tunnel. |

## Configuring Backup Bandwidth Protection

To configure backup bandwidth protection, enter the following commands.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **tunnel mpls traffic-eng-fast-reroute [bw-protect]**
4. **mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]**

## DETAILED STEPS

|        |                                                                                |                                                                                                                   |
|--------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters interface configuration mode.                                                                              |

|               |                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <pre>tunnel mpls traffic-eng fast-reroute [bw-protect]</pre> <p><b>Example:</b><br/>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect</p>                                | <p>Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.</p> <ul style="list-style-type: none"> <li>The <b>bw-protect</b> keyword gives an LSP priority for using backup tunnels with bandwidth protection. Enters global configuration mode.</li> </ul> |
| <b>Step 4</b> | <pre>mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]</pre> <p><b>Example:</b><br/>Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw</p> | <p>Changes the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.</p>                                                                                                                                          |

## Configuring an Interface for Fast Link and Node Failure Detection

To configure an interface for fast link and node failure detection, enter the following commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **pos ais-shut**
5. **pos report** {b1-tca | b2-tca | b3-tca | lais | lrldi | pais | plop | prdi | rdool | sd-ber | sf-ber | slof | slos}

### DETAILED STEPS

|               |                                                                                                 |                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                  | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p>             | <p>Enters global configuration mode.</p>                                                                                |
| <b>Step 3</b> | <pre>interface type slot/port</pre> <p><b>Example:</b><br/>Router(config)# interface pos0/0</p> | <p>Configures an interface type and enters interface configuration mode.</p>                                            |

|               |                                                                                                                                                                                           |                                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <pre>pos ais-shut</pre> <p><b>Example:</b><br/>Router(config-if)# pos ais-shut</p>                                                                                                        | Sends the line alarm indication signal (LAIS) when the POS interface is placed in any administrative shutdown state. |
| <b>Step 5</b> | <pre>pos report {b1-tca   b2-tca   b3-tca   lais   lrdi   pais   plop   prdi   rdool   sd-ber   sf-ber   slof   slos}</pre> <p><b>Example:</b><br/>Router(config-if)# pos report lrdi</p> | Permits selected SONET alarms to be logged to the console for a POS interface.                                       |

## Verifying That Fast Reroute Is Operational

To verify that FRR can function, perform the following steps.

### SUMMARY STEPS



#### Note

To determine if FRR has been configured correctly, perform Steps 1 and 2.



#### Note

If you created LSPs and performed the required configuration tasks but do not have operational backup tunnels (that is, the backup tunnels are not up or the LSPs are not associated with those backup tunnels), perform Step 3.

1. **show mpls traffic-eng tunnels brief**
2. **show ip rsvp sender detail**
3. **show mpls traffic-eng fast-reroute database**
4. **show mpls traffic-eng tunnels backup**
5. **show mpls traffic-eng fast-reroute database**
6. **show ip rsvp reservation**

### DETAILED STEPS

#### Step 1 show mpls traffic-eng tunnels brief

Use this command to verify that backup tunnels are up:

```
Router# show mpls traffic-eng tunnels brief
```

Following is sample output from the **show mpls traffic-eng tunnels brief** command:

```
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:            running
  Forwarding:              enabled
  Periodic reoptimization:  every 3600 seconds, next in 1706 seconds
TUNNEL NAME                DESTINATION    UP IF    DOWN IF    STATE/PROT
Router_t1                  10.112.0.12    -        PO4/0/1    up/up
```

```

Router_t2                10.112.0.12      -      unknown    up/down
Router_t3                10.112.0.12      -      unknown    admin-down
Router_t1000             10.110.0.10      -      unknown    up/down
Router_t2000             10.110.0.10      -      PO4/0/1    up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails

```

## Step 2 show ip rsvp sender detail

Use this command to verify that LSPs are protected by the appropriate backup tunnels.

Following is sample output from the **show ip rsvp sender detail** command when the command is entered at the PLR before a failure.

```
Router# show ip rsvp sender detail
```

```

PATH:
Tun Dest:  10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1  LSP ID: 31
Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: Rl_t100
ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
  10.10.7.1/32, Flags:0x0 (No Local Protection)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
  10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated

```

## Step 3 show mpls traffic-eng fast-reroute database

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR node protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

```
Router# show mpls traffic-eng fast-reroute database
```

```

Tunnel head end item frr information:
Protected Tunnel      In-label  intf/label      FRR intf/label      Status
Tunnel10             Tun       pos5/0:Untagged  Tu0:12304            ready

Prefix item frr information:
Prefix              Tunnel  In-label  Out intf/label  FRR intf/label      Status
10.0.0.11/32      Tu110   Tun hd    pos5/0:Untagged  Tu0:12304            ready

LSP midpoint frr information:
LSP identifier      In-label  Out intf/label  FRR intf/label      Status
10.0.0.12 1 [459]   16        pos0/1:17       Tu2000:19            ready

```

If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table ip-address detail** command. The final line of the display will tell whether that prefix is protected:

```
Router# show mpls forwarding-table 10.0.0.11 detail
```

| Local tag                                               | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|---------------------------------------------------------|--------------------|---------------------|--------------------|--------------------|-------------|
| Tun hd                                                  | Untagged           | 10.0.0.11/32        | 48                 | pos5/0             | point2point |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22}                 |                    |                     |                    |                    |             |
| 48D18847 00016000                                       |                    |                     |                    |                    |             |
| No output feature configured                            |                    |                     |                    |                    |             |
| Fast Reroute Protection via (Tu0, outgoing label 12304) |                    |                     |                    |                    |             |

#### Step 4 show mpls traffic-eng tunnels backup

For backup tunnels to be operational, the LSP must be reroutable. At the headend of the LSP, enter the **show run int tunnel tunnel-number** command. The output should include the **tunnel mpls traffic-eng fast-reroute** command. If it does not, enter this command for the tunnel.

On the router where the backup tunnels originate, enter the **show mpls traffic-eng tunnels backup** command. Following is sample command output:

```
Router# show mpls traffic-eng tunnels backup
```

```
Router_t578
LSP Head, Tunnel578, Admin: up, Oper: up
Src 10.55.55.55, Dest 10.88.88.88, Instance 1
Fast Reroute Backup Provided:
  Protected i/fs: PO1/0, PO1/1, PO3/3
  Protected lsps: 1
  Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
LSP Head, Tunnel5710, Admin: admin-down, Oper: down
Src 10.55.55.55, Dest 10.7.7.7, Instance 0
Fast Reroute Backup Provided:
  Protected i/fs: PO1/1
  Protected lsps: 0
  Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
LSP Head, Tunnel5711, Admin up, Oper: up
Src 10.55.55.55,, Dest 10.7.7.7, Instance 1
Fast Reroute Backup Provided:
  Protected i/fs: PO1/0
  Protected lsps: 2
  Backup BW: any pool unlimited; inuse: 6010 kbps
```

The command output will allow you to verify the following:

- Backup tunnel exists—Verify that there is a backup tunnel that terminates at this LSP's NHOP or NNHOP. Look for the LSP's NHOP or NNHOP in the Dest field.
- Backup tunnel is up—To verify that the backup tunnel is up, look for “Up” in the State field.
- Backup tunnel is associated with LSP's interface—Verify that the interface for the LSP is allowed to use this backup tunnel. Look for the LSP's output interface in the “protects” field list.
- Backup tunnel has sufficient bandwidth—If you restricted the amount of bandwidth a backup tunnel can hold, verify that the backup tunnel has sufficient bandwidth to hold the LSPs that would use this backup tunnel if there is a failure. The bandwidth of an LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of the LSP. To determine the available bandwidth on a backup tunnel, look at the “cfg” and “inuse” fields. If there is insufficient backup bandwidth to



accommodate the LSPs that would use this backup tunnel in the event of a failure, create an additional backup tunnel or increase the backup bandwidth of the existing tunnel by using the **tunnel mpls traffic-eng bandwidth** command.

**Note**

To determine the sufficient amount of bandwidth, offline capacity planning may be required.

- Backup tunnel has appropriate bandwidth type—If you restricted the type of LSPs (subpool or global pool) that can use this backup tunnel, verify that the LSP is the appropriate type for the backup tunnel. The type of the LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of this LSP. If this line contains the word “subpool”, then it uses sub-pool bandwidth; otherwise, it uses global pool bandwidth. Verify that the type matches the type the backup tunnel can hold by looking in the output of the **tunnel mpls traffic-eng bandwidth** command.

You also can enable debug by entering the **debug ip rsvp fast-reroute** command and the **debug mpls traffic-eng fast-reroute** command on the router that is the headend of the backup tunnel. Then do the following:

1. Enter the **shutdown** command for the primary tunnel.
2. Enter the **no shutdown** command for the primary tunnel.
3. View the debug output.

**Step 5** **show mpls traffic-eng fast-reroute database**

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR node protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

```
Router# show mpls traffic-eng fast-reroute database
```

```
Tunnel head end item frr information:
```

| Protected Tunnel | In-label | intf/label      | FRR intf/label | Status |
|------------------|----------|-----------------|----------------|--------|
| Tunnell0         | Tun      | pos5/0:Untagged | Tu0:12304      | ready  |

```
Prefix item frr information:
```

| Prefix       | Tunnel | In-label | Out intf/label  | FRR intf/label | Status |
|--------------|--------|----------|-----------------|----------------|--------|
| 10.0.0.11/32 | Tu10   | Tun hd   | pos5/0:Untagged | Tu0:12304      | ready  |

```
LSP midpoint frr information:
```

| LSP identifier    | In-label | Out intf/label | FRR intf/label | Status |
|-------------------|----------|----------------|----------------|--------|
| 10.0.0.12 1 [459] | 16       | pos0/1:17      | Tu2000:19      | ready  |

**Note**

If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table ip-address detail** command. The final line of the display will tell whether that prefix is protected:

```
Router# show mpls forwarding-table 10.0.0.11 detail
```

| Local tag                               | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|-----------------------------------------|--------------------|---------------------|--------------------|--------------------|-------------|
| Tun hd                                  | Untagged           | 10.0.0.11/32        | 48                 | pos5/0             | point2point |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22} |                    |                     |                    |                    |             |
| 48D18847 00016000                       |                    |                     |                    |                    |             |
| No output feature configured            |                    |                     |                    |                    |             |

Fast Reroute Protection via (Tu0, outgoing label 12304)

### Step 6 show ip rsvp reservation

Following is sample output from the **show ip rsvp reservation** command entered at the headend of a primary LSP. Entering the command at the headend of the primary LSP shows, among other things, the status of FRR (that is, local protection) at each hop this LSP traverses. The per-hop information is collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

Router# **show ip rsvp reservation detail**

```
Reservation:
  Tun Dest: 10.1.1.1  Tun ID: 1  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 104
  Next Hop: 172.17.1.2 on POS1/0
  Label: 18 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
RRO:
  172.18.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 18
  172.19.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 16
  172.19.1.2/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 0
  Resv ID handle: CD000404.
  Policy: Accepted. Policy source(s): MPLS/TE
```

Notice the following about the primary LSP:

- It has protection that uses a NHOP backup tunnel at its first hop.
- It has protection and is actively using an NHOP backup tunnel at its second hop.
- It has no local protection at its third hop.

The RRO display shows the following information for each hop:

- Whether local protection is available (that is, whether the LSP has selected a backup tunnel)
- Whether local protection is in use (that is, whether the LSP is currently using its selected backup tunnel)
- Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel
- Whether the backup tunnel used at this hop provides bandwidth protection

## Troubleshooting Tips

This section describes the following:

- [LSPs Do Not Become Active; They Remain Ready](#)
- [Primary Tunnel Does Not Select Backup Tunnel That Is Up](#)
- [Enhanced RSVP Commands Display Useful Information](#)
- [RSVP Hello Detects When a Neighboring Node Is Not Reachable](#)
- [Hello Instances Have Not Been Created](#)
- [“No entry at index” \(error may self-correct, RRO may not yet have propagated from downstream node of interest\)” Error Message Is Printed at the Point of Local Repair](#)

- “Couldn’t get rsbs” (error may self-correct when Resv arrives)” Error Message Is Printed at the Point of Local Repair

### LSPs Do Not Become Active; They Remain Ready

At a PLR, LSPs transition from Ready to Active if one of the following events occurs:

- Primary interface goes down—If the primary interface (LSP’s outbound interface) goes down and the LSP is ready to use a backup tunnel, the LSP will transition to the active state causing its data to flow over the backup tunnel. On some platforms and interface types (for example, GSR POS interfaces), there is fast interface-down logic that detects this event very quickly. On other platforms where this logic does not exist, detection time is slower. On such platforms, it may be desirable to enable RSVP Hello (see the next bulleted item, “Hellos detect next hop is down”).
- Hellos detect next hop is down—If Hellos are enabled on the primary interface (LSP’s outbound interface), and the LSP’s next hop is no longer reachable, the next hop is declared down. This event will cause the LSP to begin actively using its backup tunnel. Notice that a next hop will be declared down even if the primary interface does not go down. For example, if the next hop stops responding due to a reboot or software or hardware problem, Hellos will trigger the LSPs using this next hop to switch to their backup tunnels. Hellos can also help trigger FRR on interfaces such as Gigabit Ethernet where the interface remains up but is unusable (due to lack of link-layer liveness detection mechanisms).

### Primary Tunnel Does Not Select Backup Tunnel That Is Up

If a backup tunnel is up, but it is not selected as a backup tunnel by the primary tunnel (LSP), enter the following commands for the backup tunnel:

- **shutdown**
- **no shutdown**

**Note** If you change the status of a backup tunnel, the backup tunnel selection algorithm is rerun for the backup tunnel. LSPs that have currently selected (that is, are ready to use) that backup tunnel will be disassociated from it, and then reassociated with that backup tunnel or another backup tunnel. This is generally harmless and usually results in mapping the same LSPs to that backup tunnel. However, if any LSPs are actively using that backup tunnel, shutting down the backup tunnel will tear down those LSPs.

### Enhanced RSVP Commands Display Useful Information

The following RSVP commands have been enhanced to display information that can be helpful when you are examining the FRR state or troubleshooting FRR:

- **show ip rsvp request**—Displays upstream reservation state (that is, information related to the Resv messages that this node will send upstream).
- **show ip rsvp reservation**—Displays information about Resv messages received.
- **show ip rsvp sender**—Displays information about path messages being received.

These commands show control plane state; they do not show data state. That is, they show information about RSVP messages (Path and Resv) used to signal LSPs. For information about the data packets being forwarded along LSPs, use the **show mpls forwarding** command.

### RSVP Hello Detects When a Neighboring Node Is Not Reachable

The RSVP Hello feature enables RSVP nodes to detect when a neighboring node is not reachable. Use this feature when notification of link-layer failures is not available and unnumbered links are not used, or when the failure detection mechanisms provided by the link layer are not sufficient for timely node failure detection. Hello must be configured both globally on the router and on the specific interface to be operational.

### Hello Instances Have Not Been Created

If Hello instances have not been created, do the following:

- Determine if RSVP Hello has been enabled globally on the router. Enter the **ip rsvp signalling hello** (configuration) command.
- Determine if RSVP Hello has been enabled on an interface that the LSPs traverse. Enter the **ip rsvp signalling hello** (interface) command.
- Verify that at least one LSP has a backup tunnel by displaying the output of the **show ip rsvp sender** command. A value of “Ready” indicates that a backup tunnel has been selected.

### “No entry at index” (error may self-correct, RRO may not yet have propagated from downstream node of interest) Error Message Is Printed at the Point of Local Repair

FRR relies on a RRO in Resv messages arriving from downstream. Routers receiving path messages with the SESSION\_ATTRIBUTE bit indicating that the LSP is fast-reroutable should include an RRO in the corresponding Resv messages.

If an LSP is configured for FRR, but the Resv arriving from a downstream router contains an incomplete RRO, the “No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)” message is printed. An incomplete RRO is one in which the NHOP or the NNHOP did not include an entry in the RRO.

This error typically means that backup tunnels to the NHOP or the NNHOP cannot be selected for this LSP because there is insufficient information about the NHOP or NNHOP due to the lack of an RRO entry.

Occasionally there are valid circumstances in which this situation occurs temporarily and the problem is self-corrected. If subsequent Resv messages arrive with a complete RRO, ignore the error message.

To determine whether the error has been corrected, display the RRO in Resv messages by entering the **clear ip rsvp hello instance counters** command. Use an output filter keyword to display only the LSP of interest.

### “Couldn’t get rsbs” (error may self-correct when Resv arrives) Error Message Is Printed at the Point of Local Repair

The PLR cannot select a backup tunnel for an LSP until a Resv message has arrived from downstream.

When this error occurs, it typically means that something is wrong. For example, no reservation exists for this LSP. You can troubleshoot this problem by using the **debug ip rsvp reservation** command to enable debug.

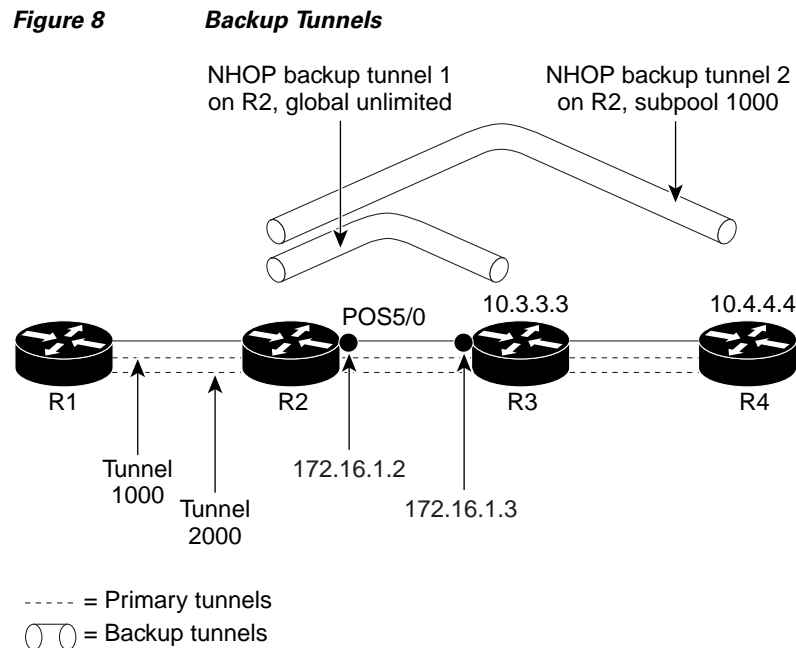
Occasionally there are valid circumstances in which this error message occurs and there is no need for concern. One such circumstance is when an LSP experiences a change before any Resv message has arrived from downstream. Changes can cause a PLR to try to select a backup tunnel for an LSP, and the selection will fail (causing this error message) if no Resv message has arrived for this LSP.

# Configuration Examples for MPLS Traffic Engineering—Fast Reroute (FRR) Link and Node Protection

This section provides the following configuration examples:

- [Enabling Fast Reroute for all Tunnels: Example, page 31](#)
- [Creating an NHOP Backup Tunnel: Example, page 32](#)
- [Creating an NNHOP Backup Tunnel: Example, page 32](#)
- [Assigning Backup Tunnels to a Protected Interface: Example, page 32](#)
- [Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example, page 33](#)
- [Configuring Backup Bandwidth Protection: Example, page 33](#)
- [Configuring an Interface for Fast Link and Node Failure Detection: Example, page 33](#)
- [Configuring RSVP Hello and POS Signals: Example, page 33](#)

The examples relate to the illustration shown in [Figure 8](#).



## Enabling Fast Reroute for all Tunnels: Example

On router R1, enter interface configuration mode for each tunnel to be protected (Tunnel 1000 and Tunnel 2000). Enable these tunnels to use a backup tunnel in case of a link or node failure along their paths.

Tunnel 1000 will use 10 units of bandwidth from the subpool.

Tunnel 2000 will use five units of bandwidth from the global pool. The “bandwidth protection desired” bit has been set by specifying **bw-prot** in the **tunnel mpls traffic-eng fast-reroute** command.

```
Router(config)# interface Tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10

Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```

## Creating an NHOP Backup Tunnel: Example

On router R2, create an NHOP backup tunnel to R3. This backup tunnel should avoid using the link 172.1.1.2.

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 172.1.1.2
Explicit Path name avoid-protected-link:
___1: exclude-address 172.1.1.2
Router(cfg-ip-expl-path)# end

Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link
```

## Creating an NNHOP Backup Tunnel: Example

On router R2, create an NNHOP backup tunnel to R4. This backup tunnel should avoid R3.

```
Router(config)# ip explicit-path name avoid-protected-node
Router(cfg-ip-expl-path)# exclude-address 10.3.3.3
Explicit Path name avoid-protected-node:
___1: exclude-address 10.3.3.3
Router(cfg-ip-expl-path)# end

Router(config)# interface Tunnel 2
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.4.4.4
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-node
```

## Assigning Backup Tunnels to a Protected Interface: Example

On router R2, associate both backup tunnels with interface POS 5/0:

```
Router(config)# interface POS 5/0
Router(config-if)# mpls traffic-eng backup-path tunnel 1
Router(config-if)# mpls traffic-eng backup-path tunnel 2
```

## Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example

Backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. It does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel 1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited

Router(config)# interface Tunnel 2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```

## Configuring Backup Bandwidth Protection: Example

In the following example, backup bandwidth protection is configured:



**Note**

This global configuration is required only to change the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

## Configuring an Interface for Fast Link and Node Failure Detection: Example

In the following example, pos ais-shut is configured:

```
Router(config)# interface pos 0/0
Router(config-if)# pos ais-shut
```

In the following example, report lrdi is configured on OS interfaces:

```
Router(config)# interface pos 0/0
Router(config-if)# pos report lrdi
```

## Configuring RSVP Hello and POS Signals: Example

Hello must be configured both globally on the router and on the specific interface on which you need FRR protection. To configure Hello, use the following configuration commands:

- **ip rsvp signalling hello** (configuration)—Enables Hello globally on the router.
- **ip rsvp signalling hello** (interface)—Enables Hello on an interface where you need FRR protection.

The following configuration commands are optional:

- **ip rsvp signalling hello dscp**—Sets the differentiated services code point (DSCP) value that is in the IP header of the Hello message.
- **ip rsvp signalling hello refresh misses**—Specifies how many acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
- **ip rsvp signalling hello refresh interval**—Configures the Hello request interval.
- **ip rsvp signalling hello statistics**—Enables Hello statistics on the router.

For configuration examples, see the Hello command descriptions in the “Command Reference” section of *MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support*, Release 12.0(24)S.

To configure POS signaling for detecting FRR failures, enter the **pos report all** command or enter the following commands to request individual reports:

```
pos ais-shut
pos report rdool
pos report lais
pos report lrldi
pos report pais
pos report prdi
pos report sd-ber
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—Fast Reroute Link and Node Protection feature.

## Related Documents

| Related Topic                               | Document Title                                                                                                             |
|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| IS-IS                                       | <a href="#">Cisco IOS IP Routing Protocols Command Reference</a><br><a href="#">Configuring a Basic IS-IS Network</a>      |
| Link protection                             | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a>    |
| Shared risk link groups                     | <a href="#">MPLS Traffic Engineering: Shared Risk Link Groups</a><br><a href="#">MPLS Traffic Engineering: Inter-AS TE</a> |
| FRR protection of TE LSPs from SRLG failure | <a href="#">MPLS Traffic Engineering: Shared Risk Link Groups</a>                                                          |
| MPLS traffic engineering commands           | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                  |
| Configuration of MPLS TE tunnels            | <a href="#">MPLS Traffic Engineering: Interarea Tunnels</a>                                                                |
| OSPF                                        | <a href="#">Cisco IOS IP Routing Protocols Command Reference</a><br><a href="#">Configuring OSPF</a>                       |
| RSVP                                        | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>                                                   |



## Standards

| Standards                                   | Title                                                     |
|---------------------------------------------|-----------------------------------------------------------|
| draft-ietf-mpls-rsvp-lsp-fastreroute-04.txt | <i>Fast ReRoute Extensions to RSVP-TE for LSP Tunnels</i> |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                        | Title                                                     |
|---------------------------------------------|-----------------------------------------------------------|
| draft-ietf-mpls-rsvp-lsp-fastreroute-06.txt | <i>Fast Reroute Extensions to RSVP-TE for LSP Tunnels</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **clear ip rsvp hello instance counters**
- **clear ip rsvp hello instance statistics**
- **clear ip rsvp hello statistics**
- **debug ip rsvp hello**
- **ip rsvp signalling hello (configuration)**
- **ip rsvp signalling hello (interface)**
- **ip rsvp signalling hello dscp**
- **ip rsvp signalling hello refresh interval**
- **ip rsvp signalling hello refresh misses**
- **ip rsvp signalling hello statistics**
- **mpls traffic-eng backup-path tunnel**
- **mpls traffic-eng fast-reroute backup-prot-preemption**
- **mpls traffic-eng fast-reroute timers**
- **show ip rsvp fast bw-protect**
- **show ip rsvp fast detail**
- **show ip rsvp hello**
- **show ip rsvp hello instance detail**
- **show ip rsvp hello instance summary**
- **show ip rsvp hello statistics**
- **show ip rsvp interface detail**
- **show ip rsvp request**
- **show ip rsvp reservation**
- **show ip rsvp sender**
- **show mpls traffic tunnel backup**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng tunnels**
- **show mpls traffic-eng tunnels summary**
- **tunnel mpls traffic-eng backup-bw**
- **tunnel mpls traffic-eng fast-reroute**

# Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

| Feature Name                                                   | Releases                                                                                                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering—Fast Reroute Link and Node Protection | 12.0(10)ST<br>12.0(16)ST<br>12.0(22)S<br>12.0(23)S<br>12.0(24)S<br>12.0(29)S<br>12.2(33)SRA<br>12.4(20)T | <p>The MPLS Traffic Engineering—Fast Reroute Link and Node Protection feature supports link protection (backup tunnels that bypass only a single link of the label-switched path (LSP), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following FRR features: backup tunnel support, backup bandwidth protection, and RSVP Hellos.</p> <p>In 12.0(10)ST, the Fast Reroute Link Protection feature was introduced.</p> <p>In 12.0(16)ST, Link Protection for Cisco series 7200 and 7500 platforms was added.</p> <p>In 12.0(22)S, Fast Reroute enhancements were added.</p> <p>In 12.0(23)S, the <b>show mpls traffic-eng fast-reroute database</b> command was revised.</p> <p>In 12.0(24)S, support for the Cisco 10720 Internet router and the Cisco 12000 series router engine 3 was added.</p> <p>In 12.0(29)S, backup bandwidth protection was added.</p> <p>In 12.2(33)SRA, the commands were integrated into this release.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> |

**Table 3**      *Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>The following commands were introduced or modified:</p> <p><b>clear ip rsvp hello instance counters, clear ip rsvp hello instance statistics, clear ip rsvp hello statistics, debug ip rsvp hello, ip rsvp signalling hello (configuration), ip rsvp signalling hello (interface), ip rsvp signalling hello dscp, ip rsvp signalling hello refresh interval, ip rsvp signalling hello refresh misses, ip rsvp signalling hello statistics, mpls traffic-eng backup-path tunnel, mpls traffic-eng fast-reroute backup-prot-preemption, mpls traffic-eng fast-reroute timers, show ip rsvp fast bw-protect, show ip rsvp fast detail, show ip rsvp hello, show ip rsvp hello instance detail, show ip rsvp hello instance summary, show ip rsvp hello statistics, show ip rsvp interface detail, show ip rsvp request, show ip rsvp reservation, show ip rsvp sender, show mpls traffic tunnel backup, show mpls traffic-eng fast-reroute database, show mpls traffic-eng tunnels, show mpls traffic-eng tunnels summary, tunnel mpls traffic-eng backup-bw, tunnel mpls traffic-eng fast-reroute.</b></p> |

# Glossary

**backup bandwidth**—The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

**backup tunnel**—An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

**bandwidth**—The available traffic capacity of a link.

**Cisco Express Forwarding**—A means for accelerating the forwarding of packets within a router, by storing route lookup.

**enterprise network**—A large and diverse network connecting most major points in a company or other organization.

**Fast Reroute**—Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

**global pool**—The total bandwidth allocated to an MPLS traffic engineering link or node.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**instance**—A Hello instance implements the RSVP Hello extensions for a given router interface address and remote IP address. Active Hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**interface**—A network connection.

**Intermediate System-to-Intermediate System**—IS-IS. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

**link**—A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**limited backup bandwidth**—Backup tunnels that provide bandwidth protection.

**load balancing**—A configuration technique that shifts traffic to an alternative link if a certain threshold is exceeded on the primary link. Load balancing is similar to redundancy in that if an event causes traffic to shift directions, alternative equipment must be present in the configuration. In load balancing, the alternative equipment is not necessarily redundant equipment that operates only in the event of a failure.

**LSP**—label-switched path. A connection between two routers in which MPLS forwards the packets.

**merge point**—The backup tunnel's tail.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**MPLS global label allocation**—There is one label space for all interfaces in the router. For example, label 100 coming in one interface is treated the same as label 100 coming in a different interface.

**NHOP**—next hop. The next downstream node along an LSP's path.

**NHOP backup tunnel**—next-hop backup tunnel. Backup tunnel terminating at the LSP's next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

**NNHOP**—next-next hop. The node after the next downstream node along an LSP's path.

**NNHOP backup tunnel**—next-next-hop backup tunnel. Backup tunnel terminating at the LSP's next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.

**node**—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.

**OSPF**—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**primary LSP**—The last LSP originally signaled over the protected interface before the failure. The primary LSP is the LSP before the failure.

**primary tunnel**—Tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**promotion**—Conditions, such as a new backup tunnel comes up, cause a reevaluation of a backup tunnel that was chosen for an LSP. If the reevaluation is successful, it is called a promotion.

**protected interface**—An interface that has one or more backup tunnels associated with it.

**redundancy**—The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

**RSVP**—Resource Reservation Protocol. A protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

**scalability**—An indicator showing how quickly some measure of resource usage increases as a network gets larger.

**SRLG**—shared risk link group. Sets of links that are likely to go down together.

**state**—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**sub-pool**—The more restrictive bandwidth in an MPLS traffic engineering link or node. The subpool is a portion of the link or node's overall global pool bandwidth.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**topology**—The physical arrangement of network nodes and media within an enterprise networking structure.

**tunnel**—Secure communications path between two peers, such as two routers.

**unlimited backup bandwidth**—Backup tunnels that provide no bandwidth (best-effort) protection (that is, they provide best-effort protection).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLNNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream,

Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2003–2009 Cisco Systems, Inc. All rights reserved.







# MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

---

**First Published: October 10, 2004**

**Last Updated: February 27, 2009**

The MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) feature provides the following Fast Reroute (FRR) capabilities:

- Backup tunnel that terminates at the next-next hop router to protect both the downstream link and node in order to protect link and node failures. There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. A backup tunnel is scalable because it can protect multiple label switched paths (LSPs) and multiple interfaces.
- Backup bandwidth protection allows a priority to be assigned to backup tunnels for LSPs carrying certain kinds of data (such as voice).
- Fast Tunnel Interface Down detection, which forces a “generic” interface tunnel (not specifically a Fast Reroute tunnel) to become disabled immediately if the headend router detects a failed link on an LSP.
- Resource Reservation Protocol (RSVP) Hellos, which are used to accelerate the detection of node failures.



## Note

If the Multiprotocol Label Switching (MPLS) TE FRR Link Protection feature is planned to be used in releases earlier than Cisco IOS Release 12.0(24)S, contact the Cisco Technical Assistance Center for important deployment and upgrade information.

---

For information about shared risk link groups (SRLGs), which are sets of links that are likely to go down together, refer to [MPLS Traffic Engineering: Shared Risk Link Groups](#).



---

**Americas Headquarters:**

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

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#)” section on page 39.

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

## Contents

- [Prerequisites for MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 2
- [Restrictions for MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 3
- [Information About MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 3
- [How to Configure MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 18
- [Configuration Examples for MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 33
- [Additional References](#), page 37
- [Command Reference](#), page 38
- [Feature Information for MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#), page 39
- [Glossary](#), page 41

## Prerequisites for MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

Your network must support the following Cisco IOS features in order to support features described in this document:

- IP Cisco Express Forwarding
- MPLS

Your network must support at least one of the following protocols:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

# Restrictions for MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

- Interfaces must use MPLS Global Label Allocation.
- Backup tunnel headend and tailend routers must implement FRR as described in this document.
- Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.
- LSPs that are actively using backup tunnels are not considered for promotion. So, if an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.

## Information About MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

To configure the MPLS TE Link and Node Protection with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) feature, you need to understand the following concepts:

- [Fast Reroute, page 3](#)
- [Link Protection, page 4](#)
- [Node Protection, page 4](#)
- [Bandwidth Protection, page 5](#)
- [Fast Tunnel Interface Down Detection, page 5](#)
- [RSVP Hello, page 5](#)
- [Features of MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\), page 7](#)
- [Fast Reroute Operation, page 9](#)

## Fast Reroute

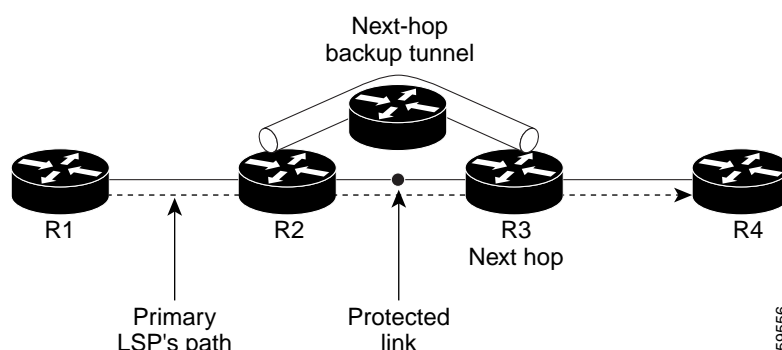
Fast Reroute (FRR) is a mechanism for protecting MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

For information about how FRR protects TE LSPs from shared risk link group (SRLG) failure, refer to *MPLS Traffic Engineering: Shared Risk Link Groups*.

## Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide Link Protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure. [Figure 1](#) illustrates an NHOP backup tunnel.

**Figure 1** *NHOP Backup Tunnel*

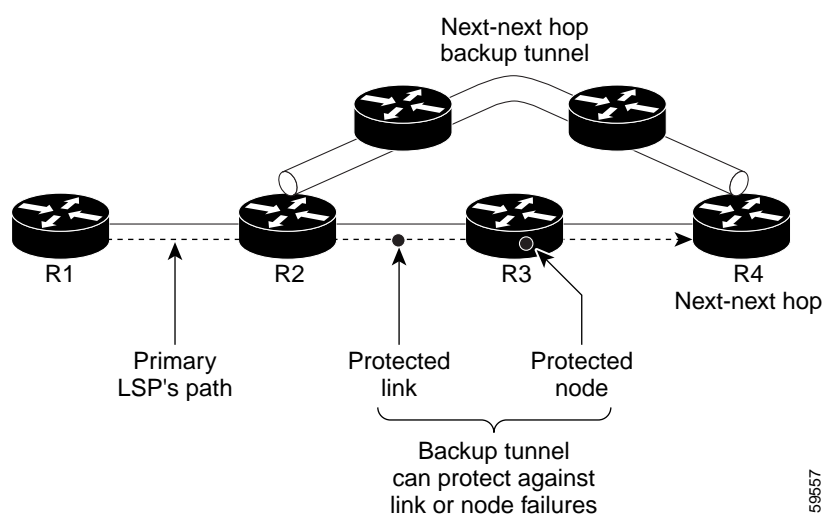


## Node Protection

FRR provides Node Protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link in addition to the node.

[Figure 2](#) illustrates an NNHOP backup tunnel.

**Figure 2** *NNHOP Backup Tunnel*



If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes include the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.
- Primary LSP is modified so that FRR is disabled. (The **no mpls traffic-eng fast-reroute** command is entered.)

## Bandwidth Protection

NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected. For information about mapping tunnels and assigning backup bandwidth, see the [“Backup Tunnel Selection Procedure” section on page 11](#).

LSPs that have the “bandwidth protection desired” bit set have a higher right to select backup tunnels that provide bandwidth protection; that is, those LSPs can preempt other LSPs that do not have that bit set. For more information, see the [“Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection” section on page 9](#).

## Fast Tunnel Interface Down Detection

Fast Tunnel Interface Down detection forces a “generic” interface tunnel (not specifically a Fast Reroute tunnel) to become disabled immediately if the headend router detects a failed link on an LSP.

This feature is configured with the **tunnel mpls traffic-eng interface down delay** command. If this feature is not configured, there is a delay before the tunnel becomes unoperational and before the traffic uses an alternative path chosen by the headend/midpoint router to forward the traffic. This is acceptable for data traffic, but not for voice traffic because it relies on the TE tunnel to go down as soon as the LSP goes down.

## RSVP Hello

RSVP Hellos are described in the following sections:

- [RSVP Hello Operation, page 6](#)
- [Hello Instance, page 6](#)
- [Hello Commands, page 7](#)

## RSVP Hello Operation

- `ip rsvp signalling hello refresh interval`
- `ip rsvp signalling hello refresh misses`



### Note

## Hello Instance

- 
- 

### Active Hello Instances

### Passive Hello Instances

## Hello Commands

*Traffic Engineering—RSVP Hello State Timer*

## Features of MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

- 
- 
- 

## Backup Tunnel Support

- 
- 
- 

**Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR**

**Multiple Backup Tunnels Can Protect the Same Interface**

- Redundancy—If one backup tunnel is down, other backup tunnels protect LSPs.

- Increased backup capacity—If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels). For a more detailed explanation, see the [“Backup Tunnel Selection Procedure” section on page 11](#).

Examples are shown in the [“Backup Tunnels Terminating at Different Destinations” section on page 10](#) and the [“Backup Tunnels Terminating at the Same Destination” section on page 11](#).

### Scalability

A backup tunnel is scalable because it can protect multiple LSPs and multiple interfaces. It provides many-to-one (N:1) protection, which has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

Example of 1:1 protection: When 5,000 backup tunnels protect 5,000 LSPs, each router along the backup path must maintain state for an additional 5,000 tunnels.

Example of N:1 protection: When one backup tunnel protects 5,000 LSPs, each router along the backup path maintains one additional tunnel.

## Backup Bandwidth Protection

Backup bandwidth protection has the following capabilities:

- [Bandwidth Protection on Backup Tunnels, page 8](#)
- [Bandwidth Pool Specifications for Backup Tunnels, page 8](#)
- [Semidynamic Backup Tunnel Paths, page 8](#)
- [Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection, page 9](#)

### Bandwidth Protection on Backup Tunnels

Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.

### Bandwidth Pool Specifications for Backup Tunnels

You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using subpool bandwidth can use them or only LSPs that use global pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could (optionally) not provide bandwidth protection.

### Semidynamic Backup Tunnel Paths

The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature that was added in Release 12.0(14)ST. Using this feature, semidynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semidynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.



**Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection**

In case there are not enough NHOP or NNHOP backup tunnels or they do not have enough backup bandwidth to protect all LSPs, you can give an LSP priority in obtaining backup tunnels with bandwidth protection. This is especially useful if you want to give LSPs carrying voice a higher priority than those carrying data.

To activate this feature, enter the **tunnel mpls traffic-eng fast-reroute bw-protect**

*receive*

*chance*

**Fast Reroute Operation**

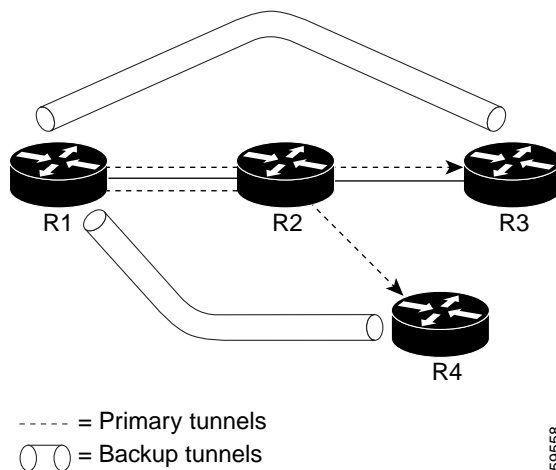
- 
- 
- 
- 
- 
- 
- 
- 
- 
-

## Fast Reroute Activation

- 
- 
- 

## Backup Tunnels Terminating at Different Destinations

**Figure 3** Backup Tunnels that Terminate at Different Destinations

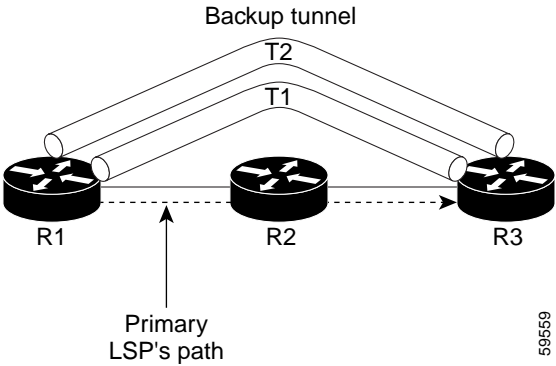


59558

- 
-

# Backup Tunnels Terminating at the Same Destination

Figure 4 Backup Tunnels that Terminate at the Same Destination



## Backup Tunnel Selection Procedure

- 
- 
- fast-reroute tunnel mpls traffic-eng
- 
- 
- mpls traffic-eng backup-path
-

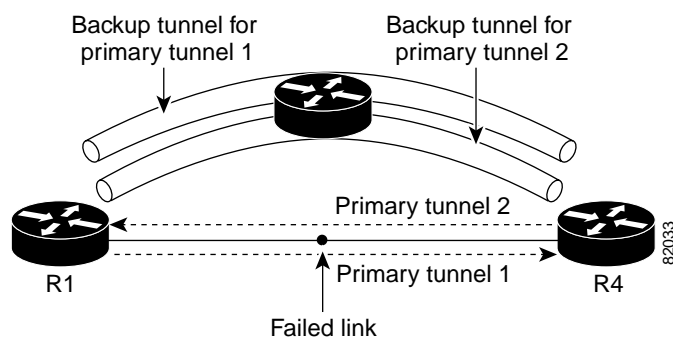
- 
- 

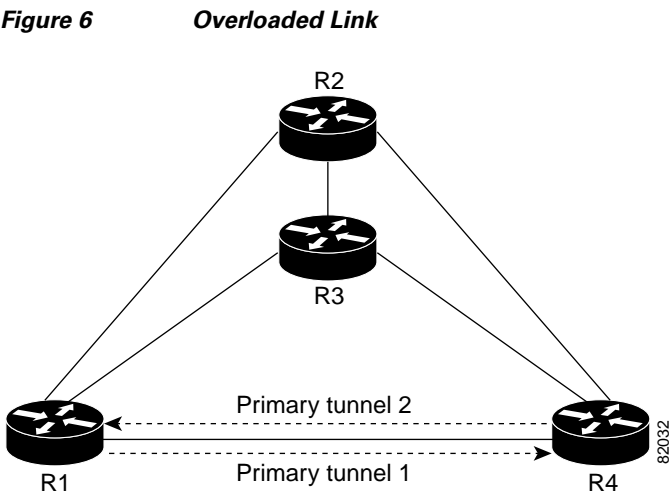
## Bandwidth Protection

- 
- 

## Load Balancing on Limited-bandwidth Backup Tunnels

**Figure 5** *Backup Tunnels Share a Link*





**Load Balancing on Unlimited-bandwidth Backup Tunnels**

**Pool Type and Backup Tunnels**

**Tunnel Selection Priorities**

- 
- 
- 

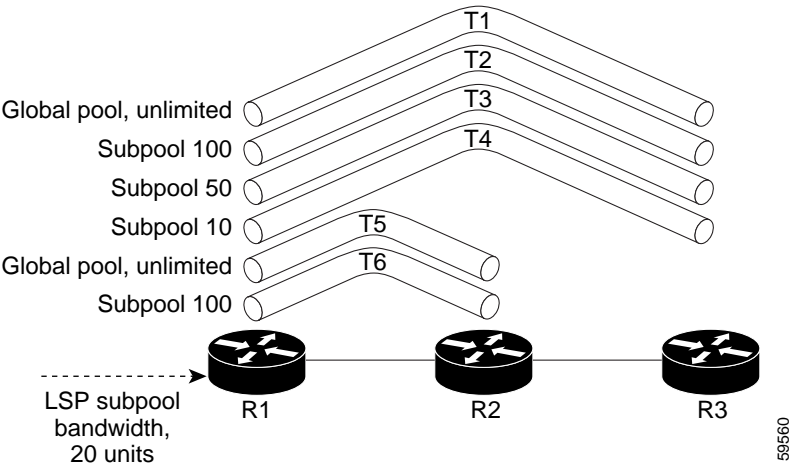
**NHOP Versus NNHOP Backup Tunnels**

Table 1 Tunnel Selection Priorities

| Preference | Backup Tunnel Destination | Bandwidth Pool | Bandwidth Amount |
|------------|---------------------------|----------------|------------------|
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |
|            |                           |                |                  |

  
Note

Figure 7 Choosing from Among Multiple Backup Tunnels



- 1.
- 2.
- 3.

4.

5.

Promotion

1.

2.

3.

4.

mpls traffic-eng fast-reroute timers

Backup Protection Preemption Algorithms

- 
- 
- 
- 

mpls traffic-eng fast-reroute

backup-prot-preemption optimize-bw

Bandwidth Protection Considerations

Bandwidth Protection Methods

| Method | Advantages | Disadvantages |
|--------|------------|---------------|
|        |            |               |
|        |            |               |
|        |            |               |

- 
- [Using Backup Tunnels Signaled with Zero Bandwidth, page 17](#)

Using Backup Tunnels with Explicitly Signaled Bandwidth

- 
- 

tunnel mpls traffic-eng bandwidth

tunnel mpls traffic-eng backup-bw



### Protected Bandwidth Pools and the Bandwidth Pool from Which the Backup Tunnel Reserves Its Bandwidth

#### `tunnel mpls traffic-eng bandwidth`

- 
- 



#### Note

#### `tunnel mpls traffic-eng backup-bw`

- 
- 

Bandwidth protection for 10 Kbps of subpool traffic on a given link can be achieved by any of the following combinations:

- `tunnel mpls traffic-eng bandwidth sub-pool 10`  
`tunnel mpls traffic-eng backup-bw sub-pool 10`
- `tunnel mpls traffic-eng bandwidth global-pool 10`  
`tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool unlimited`
- `tunnel mpls traffic-eng bandwidth global-pool 40`  
`tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool 30`

### Using Backup Tunnels Signaled with Zero Bandwidth

Frequently it is desirable to use backup tunnels with zero signaled bandwidth, even when bandwidth protection is required. It may seem that if no bandwidth is explicitly reserved, no bandwidth guarantees can be provided. However, that is not necessarily true.

In the following situation:

- Only link protection is desired.
- Bandwidth protection is desired only for subpool traffic.

For each protected link AB with a max reservable subpool value of  $S$ , there may be a path from node A to node B such that the difference between max reservable global and max reservable subpool is at least  $S$ . If it is possible to find such paths for each link in the network, you can establish all the backup tunnels along such paths without any bandwidth reservations. If there is a single link failure, only one backup tunnel will use any link on its path. Because that path has at least  $S$  of available bandwidth (in the global pool), assuming that marking and scheduling is configured to classify the subpool traffic into a priority queue, the subpool bandwidth is guaranteed.

The above approach allows sharing of the global pool bandwidth between backup tunnels protecting independent link failures. The backup tunnels are expected to be used for only a short period of time after a failure (until the headends of affected LSPs reroute those LSPs to other paths with available

subpool bandwidth). The probability of multiple unrelated link failures is very small (in the absence of node or SRLG failures, which result in multiple link failures). Therefore, it is reasonable to assume that link failures are in practice independent with high probability. This “independent failure assumption” in combination with backup tunnels signaled without explicit bandwidth reservation enables efficient bandwidth sharing that yields substantial bandwidth savings.

Backup tunnels protecting the subpool traffic do now draw bandwidth from any pool. Primary traffic using the global pool can use the entire global pool, and primary traffic using the subpool can use the entire subpool. Yet, subpool traffic has a complete bandwidth guarantee if there is a single link failure.

A similar approach can be used for node and SRLG protection. However, the decision of where to put the backup tunnels is more complicated because both node and SRLG failures effectively result in the simultaneous failure of several links. Therefore, the backup tunnels protecting traffic traversing all affected links cannot be computed independently of each other. The backup tunnels protecting groups of links corresponding to different failures can still be computed independently of each other, which results in similar bandwidth savings.

### Signaled Bandwidth Versus Backup Bandwidth

Backup bandwidth is used locally (by the router that is the headend of the backup tunnel) to determine which, and how many, primary LSPs can be rerouted on a particular backup tunnel. The router ensures that the combined bandwidth requirement of these LSPs does not exceed the backup bandwidth.

Therefore, even when the backup tunnel is signaled with zero bandwidth, the backup bandwidth must be configured with the value corresponding to the actual bandwidth requirement of the traffic protected by this backup tunnel. Unlike the case when bandwidth requirements of the backup tunnels are explicitly signaled, the value of the signaled bandwidth (which is zero) is not the same value as the backup bandwidth.

## How to Configure MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured.

Make sure that the following tasks have been performed before you perform the configuration tasks, but you do not have to already have configured MPLS TE tunnels:

- Enabled MPLS TE on all relevant routers and interfaces
- Configured MPLS TE tunnels

The following sections describe how to use FRR to protect LSPs in your network from link or node failures. Each task is identified as either required or optional.

- [Enabling Fast Reroute on LSPs, page 19](#) (required)
- [Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop, page 20](#) (required)
- [Assigning Backup Tunnels to a Protected Interface, page 21](#) (required)
- [Associating Backup Bandwidth and Pool Type with a Backup Tunnel, page 22](#) (optional)
- [Configuring Backup Bandwidth Protection, page 23](#) (optional)
- [Configuring an Interface for Fast Link and Node Failure Detection, page 24](#) (optional)

- [Configuring an Interface for Fast Tunnel Interface Down, page 25](#) (optional)
- [Verifying That Fast Reroute Is Operational, page 25](#) (optional)



Note

You can perform the configuration tasks in any order.



Note

An NNHOP backup tunnel must      go via the NHOP.

## Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if they have been configured as fast reroutable. To do this, enter the following commands at the headend of each LSP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **tunnel mpls traffic-eng fast-reroute [bw-protect] [node-protect]**

### DETAILED STEPS

|        | Command                                                                         | Purpose                                                                                           |
|--------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                                   | Enables privileged EXEC mode.<br><br>Enter your password if prompted.                             |
|        | <b>Example:</b><br>Router> enable                                               |                                                                                                   |
|        | <b>configure terminal</b>                                                       | Enters global configuration mode.                                                                 |
|        | Router# configure terminal                                                      |                                                                                                   |
|        | <b>interface tunnel <i>number</i></b>                                           | Enters interface configuration mode for the specified tunnel.                                     |
|        | Router(config)# interface tunnel 1000                                           |                                                                                                   |
|        | <b>tunnel mpls traffic-eng fast-reroute [bw-protect] [node-protect]</b>         | Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure. |
|        | Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect |                                                                                                   |

# Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop



Note

exclude-address

## SUMMARY STEPS

- 1. enable
- 2. configure terminal
- 3. interface tunnel
- 4. ip unnumbered *type number*  
tunnel destination *A.B.C.D*
- 6. tunnel mode mpls traffic-eng
- 7. tunnel mpls traffic-eng path-option *number* {dynamic | explicit {name *path-name*  
*path-number*}} [lockdown]
- 8. ip explicit-path name
- 9. exclude-address

## DETAILED STEPS

|        | Command  | Purpose                                                                            |
|--------|----------|------------------------------------------------------------------------------------|
| Step 1 |          | Enables privileged EXEC mode.                                                      |
|        | Example: | <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 |          | Enters global configuration mode.                                                  |
|        | Example: |                                                                                    |
| Step 3 |          | Creates a new tunnel interface and enters interface configuration mode.            |
|        | Example: |                                                                                    |

#### Step 4

|                                                                                                                                                                                                                                                                               |                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><i>type number</i></p> <p><b>Example:</b><br/>Router(config-if)# ip unnumbered loopback0</p>                                                                                                                                                                               | <p>Gives the tunnel interface an IP address that is the same as that of interface Loopback0.</p> <p>This command is not effective until Loopback0 has been configured with an IP address.</p> |
| <p><i>A.B.C.D</i></p> <p>Router(config-if)# tunnel destination 10.3.3.3</p>                                                                                                                                                                                                   | <p>Specifies the IP address of the device where the tunnel will terminate.</p> <p>That address should be the router ID of the device that is the NHOP or NNHOP of LSPs to be protected.</p>   |
| <p>Router(config-if)# tunnel mode mpls traffic-eng</p>                                                                                                                                                                                                                        | <p>Sets encapsulation mode of the tunnel to MPLS TE.</p>                                                                                                                                      |
| <p><b>tunnel mpls traffic-eng path-option</b> <i>number</i> {<b>dynamic</b>   <b>explicit</b> {<b>name</b> <i>path-name</i>   <i>path-number</i>}} [<b>lockdown</b>]</p> <p>Router(config-if)# tunnel mpls traffic-eng path-option 300 explicit name avoid-protected-link</p> |                                                                                                                                                                                               |
| <p><b>ip explicit-path name</b> <i>name</i></p> <p>Router(config)# ip explicit-path name avoid-protected-link</p>                                                                                                                                                             |                                                                                                                                                                                               |
| <p><b>exclude-address</b> <i>address</i></p> <p>Router(cfg-ip-expl-path)# exclude-address 10.3.3.3</p>                                                                                                                                                                        |                                                                                                                                                                                               |

## Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the [“Finding Feature Information”](#) section on page 2.



#### Note

You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.



|        | Command                                                                                                                         | Purpose                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                    | <ul style="list-style-type: none"><li></li></ul>                                                                                            |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                                            |                                                                                                                                             |
| Step 3 | <code>interface           slot/port</code><br><br><b>Example:</b><br>Router(config)# interface POS5/0                           | <ul style="list-style-type: none"><li><div><div></div><div><div><i>type</i></div><div><i>slot</i>   <i>port</i></div></div></div></li></ul> |
| Step 4 | <div><div></div><div><i>tunnel-id</i></div></div><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng backup-path tunnel2 | <b>Note</b>                                                                                                                                 |

## Associating Backup Bandwidth and Pool Type with a Backup Tunnel

### SUMMARY STEPS

1.
2.
3.
4.

*bandwidth*

*bandwidth*           *bandwidth*           *bandwidth*



DETAILED STEPS

|        | Command                                                                                                                                                                                                                   | Purpose                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Step 1 | <div>Example:<br/>Router&gt; enable</div>                                                                                                                                                                                 | <ul style="list-style-type: none"><li></li></ul> |
| Step 2 | <div>Example:<br/>Router# configure terminal</div>                                                                                                                                                                        |                                                  |
| Step 3 | <div><i>number</i></div> <div>Example:<br/>Router(config)# interface tunnel 2</div>                                                                                                                                       |                                                  |
| Step 4 | <div><pre>{bandwidth  <br/>[ {bandwidth   } ] [ {bandwidth  <br/>{bandwidth   } ] } [ {bandwidth  <br/>    } ]</pre></div> <div>Example:<br/>Router(config-if)# tunnel mpls traffic-eng backup-bw<br/>sub-pool 1000</div> |                                                  |

Configuring Backup Bandwidth Protection

SUMMARY STEPS

1.
2.
3. *number*
4.
5.

DETAILED STEPS

|        |                                                    |                                                  |
|--------|----------------------------------------------------|--------------------------------------------------|
| Step 1 | <div>Example:<br/>Router&gt; enable</div>          | <ul style="list-style-type: none"><li></li></ul> |
| Step 2 | <div>Example:<br/>Router# configure terminal</div> |                                                  |

|                                                                                     |                   |
|-------------------------------------------------------------------------------------|-------------------|
| <i>number</i>                                                                       |                   |
| Router(config)# interface tunnel 2                                                  |                   |
| <i>[</i> <i>          </i> <i>]</i>                                                 |                   |
| Router(config-if)# tunnel mpls traffic-eng<br>fast-reroute bw-protect               | <b>bw-protect</b> |
| <b>[optimize-bw]</b>                                                                |                   |
| Router(config)# mpls traffic-eng fast-reroute<br>backup-prot-preemption optimize-bw |                   |

Configuring an Interface for Fast Link and Node Failure Detection

SUMMARY STEPS

1.
2.
3. *type slot port*
4.
5. **b2-tca b3-tca lais lrdi pais plop prdi rdool sd-ber sf-ber slof**  
**slos**

|                                             |  |
|---------------------------------------------|--|
| <b>enable</b>                               |  |
| Router> enable                              |  |
| <b>configure terminal</b>                   |  |
| Router# configure terminal                  |  |
| <b>interface</b> <i>          </i> <i>/</i> |  |
| Router(config)# interface pos0/0            |  |



|                                                                                                                                     |  |
|-------------------------------------------------------------------------------------------------------------------------------------|--|
| <pre>pos ais-shut</pre>                                                                                                             |  |
| <pre>Router(config-if)# pos ais-shut</pre>                                                                                          |  |
| <pre>pos report {b1-tca   b2-tca   b3-tca   lais   lrdi  <br/>pais   plop   prdi   rdool   sd-ber   sf-ber   slof  <br/>slos}</pre> |  |
| <pre>Router(config-if)# pos report lrdi</pre>                                                                                       |  |

**enable**  
**configure terminal**  
**interface** *type slot/port*  
**tunnel mpls traffic-eng interface down delay** *time*

|                                                                                  |  |
|----------------------------------------------------------------------------------|--|
| <pre>enable</pre>                                                                |  |
| <pre>Router&gt; enable</pre>                                                     |  |
| <pre>configure terminal</pre>                                                    |  |
| <pre>Router# configure terminal</pre>                                            |  |
| <pre>interface /</pre>                                                           |  |
| <pre>Router(config)# interface tunnel 1000</pre>                                 |  |
| <pre>tunnel mpls traffic-eng interface down delay</pre>                          |  |
| <pre>Router(config-if)# tunnel mpls traffic-eng interface<br/>down delay 0</pre> |  |



- show mpls traffic-eng tunnels brief
- show ip rsvp sender detail
- show mpls traffic-eng fast-reroute database
- show mpls traffic-eng tunnels backup
- show mpls traffic-eng fast-reroute database
- show ip rsvp reservation

## show mpls traffic-eng tunnels brief

Router# **show mpls traffic-eng tunnels brief**

```
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:            running
  Forwarding:              enabled
  Periodic reoptimization:  every 3600 seconds, next in 1706 seconds
TUNNEL NAME                DESTINATION    UP IF    DOWN IF    STATE/PROT
Router_t1                  10.112.0.12   -        PO4/0/1    up/up
Router_t2                  10.112.0.12   -        unknown    up/down
Router_t3                  10.112.0.12   -        unknown    admin-down
Router_t1000               10.110.0.10   -        unknown    up/down
Router_t2000               10.110.0.10   -        PO4/0/1    up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

## show ip rsvp sender detail

### show ip rsvp sender detail

Router# **show ip rsvp sender detail**

```
PATH:
Tun Dest:  10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1  LSP ID: 31
Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: R1_t100
```

```

ERO: (incoming)
  10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
  10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
  10.10.7.1/32, Flags:0x0 (No Local Protection)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
  10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated

```

## show mpls traffic-eng fast-reroute database

### clear ip rsvp hello instance counters

Router# **show mpls traffic-eng fast-reroute database**

Tunnel head end item frr information:

| Protected tunnel | In-label | Out intf/label   | FRR intf/label | Status |
|------------------|----------|------------------|----------------|--------|
| Tunnel500        | Tun hd   | AT4/0.100:Untagg | Tu501:20       | ready  |

Prefix item frr information:

| Prefix      | Tunnel | In-label | Out intf/label   | FRR intf/label | Status |
|-------------|--------|----------|------------------|----------------|--------|
| 10.0.0.8/32 | Tu500  | 18       | AT4/0.100:Pop ta | Tu501:20       | ready  |
| 10.0.8.8/32 | Tu500  | 19       | AT4/0.100:Untagg | Tu501:20       | ready  |
| 10.8.9.0/24 | Tu500  | 22       | AT4/0.100:Untagg | Tu501:20       | ready  |

LSP midpoint item frr information:

| LSP identifier | In-label | Out intf/label | FRR intf/label | Status |
|----------------|----------|----------------|----------------|--------|
|----------------|----------|----------------|----------------|--------|

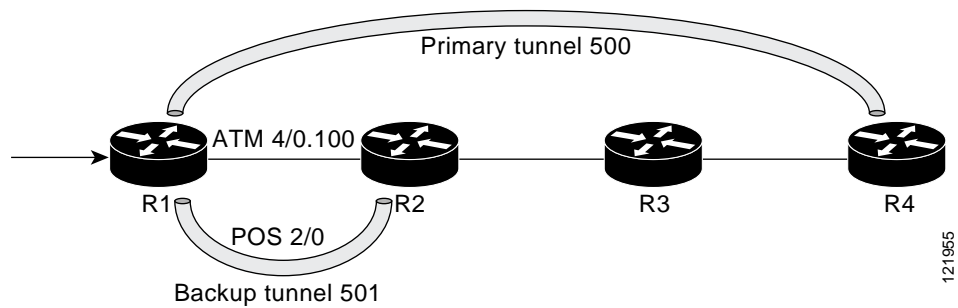
## show mpls forwarding-table ip-address detail

Router# **show mpls forwarding-table 10.0.0.11 32 detail**

| Local                                                   | Outgoing  | Prefix       | Bytes tag | Outgoing  | Next Hop    |
|---------------------------------------------------------|-----------|--------------|-----------|-----------|-------------|
| tag                                                     | tag or VC | or Tunnel Id | switched  | interface |             |
| Tun hd                                                  | Untagged  | 10.0.0.11/32 | 48        | pos5/0    | point2point |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22}                 |           |              |           |           |             |
| 48D18847 00016000                                       |           |              |           |           |             |
| No output feature configured                            |           |              |           |           |             |
| Fast Reroute Protection via (Tu0, outgoing label 12304) |           |              |           |           |             |

*primary*

**Figure 8 Protected LSPs**



```
Router# show mpls traffic-eng fast-reroute database
```

Tunnel head end item frr information:

| Protected tunnel | In-label | Out                 | intf/label | FRR   | intf/label | Status |
|------------------|----------|---------------------|------------|-------|------------|--------|
| Tunnel500        | Tu500    | hd AT4/0.100:Untagg | Tu501:20   | ready |            |        |

Prefix item frr information:

| Prefix      | Tunnel | In-label | Out              | intf/label | FRR   | intf/label | Status |
|-------------|--------|----------|------------------|------------|-------|------------|--------|
| 10.0.0.8/32 | Tu500  | 18       | AT4/0.100:Pop ta | Tu501:20   | ready |            |        |
| 10.0.8.8/32 | Tu500  | 19       | AT4/0.100:Untagg | Tu501:20   | ready |            |        |
| 10.8.9.0/24 | Tu500  | 22       | AT4/0.100:Untagg | Tu501:20   | ready |            |        |

LSP midpoint item frr information:

| LSP identifier | In-label | Out | intf/label | FRR | intf/label | Status |
|----------------|----------|-----|------------|-----|------------|--------|
|                |          |     |            |     |            |        |

```
Router# show mpls traffic-eng fast-reroute database
```

Tunnel head end item frr information:

| Protected tunnel | In-label | Out               | intf/label | FRR   | intf/label | Status |
|------------------|----------|-------------------|------------|-------|------------|--------|
| Tunnel500        | Tu500    | hd PO2/0:Untagged | Tu501:20   | ready |            |        |

Prefix item frr information:

| Prefix      | Tunnel | In-label | Out            | intf/label | FRR   | intf/label | Status |
|-------------|--------|----------|----------------|------------|-------|------------|--------|
| 10.0.0.8/32 | Tu500  | 18       | PO2/0:Pop tag  | Tu501:20   | ready |            |        |
| 10.0.8.8/32 | Tu500  | 19       | PO2/0:Untagged | Tu501:20   | ready |            |        |
| 10.8.9.0/24 | Tu500  | 22       | PO2/0:Untagged | Tu501:20   | ready |            |        |

LSP midpoint item frr information:

| LSP identifier | In-label | Out | intf/label | FRR | intf/label | Status |
|----------------|----------|-----|------------|-----|------------|--------|
|                |          |     |            |     |            |        |

**show mpls traffic-eng tunnels backup**

LSP is reroutable

show run int tunnel  
tunnel mpls traffic-eng fast-reroute

show mpls traffic-eng tunnels backup

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsps: 1
    Backup BW: any pool unlimited; inuse: 100 kbps
Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsps: 0
    Backup BW: any pool unlimited; inuse: 0 kbps
Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

traffic-eng bandwidth

tunnel mpls

mpls traffic-eng bandwidth

tunnel



tunnel mpls traffic-eng bandwidth

**debug mpls traffic-eng fast-reroute**

**debug ip rsvp fast-reroute**

**shutdown**

**no shutdown**

**show mpls traffic-eng fast-reroute database**

**clear ip rsvp hello instance counters**

Router# **show mpls traffic-eng fast-reroute database**

Tunnel head end item frr information:

| Protected Tunnel | In-label | intf/label      | FRR intf/label | Status |
|------------------|----------|-----------------|----------------|--------|
| Tunnell0         | Tun      | pos5/0:Untagged | Tu0:12304      | ready  |

Prefix item frr information:

| Prefix       | Tunnel | In-label | Out intf/label  | FRR intf/label | Status |
|--------------|--------|----------|-----------------|----------------|--------|
| 10.0.0.11/32 | Tu110  | Tun hd   | pos5/0:Untagged | Tu0:12304      | ready  |

LSP midpoint frr information:

| LSP identifier    | In-label | Out intf/label | FRR intf/label | Status |
|-------------------|----------|----------------|----------------|--------|
| 10.0.0.12 1 [459] | 16       | pos0/1:17      | Tu2000:19      | ready  |



**show mpls forwarding-table**

**detail**

Router# **show mpls forwarding-table 10.0.0.11 32 detail**

| Local                                                   | Outgoing  | Prefix       | Bytes tag | Outgoing  | Next Hop    |
|---------------------------------------------------------|-----------|--------------|-----------|-----------|-------------|
| tag                                                     | tag or VC | or Tunnel Id | switched  | interface |             |
| Tun hd                                                  | Untagged  | 10.0.0.11/32 | 48        | pos5/0    | point2point |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22}                 |           |              |           |           |             |
| 48D18847 00016000                                       |           |              |           |           |             |
| No output feature configured                            |           |              |           |           |             |
| Fast Reroute Protection via (Tu0, outgoing label 12304) |           |              |           |           |             |

**show ip rsvp reservation**

Following is sample output from the **show ip rsvp reservation** command entered at the headend of a primary LSP. Entering the command at the head-end of the primary LSP

collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

Router# **show ip rsvp reservation detail**

Reservation:

Tun Dest: 10.1.1.1 Tun ID: 1 Ext Tun ID: 10.1.1.1  
Tun Sender: 10.1.1.1 LSP ID: 104  
Next Hop: 10.1.1.2 on POS1/0  
Label: 18 (outgoing)

Reservation Style is Shared-Explicit, QoS Service is Controlled-Load  
Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes  
Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes  
RRO:  
  10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)  
    Label subobject: Flags 0x1, C-Type 1, Label 18  
  10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)  
    Label subobject: Flags 0x1, C-Type 1, Label 16  
  10.1.1.2/32, Flags:0x0 (No Local Protection)  
    Label subobject: Flags 0x1, C-Type 1, Label 0  
Resv ID handle: CD000404.  
Policy: Accepted. Policy source(s): MPLS/TE

Notice the following about the primary LSP:

It has protection that uses a NHOP backup tunnel at its first hop.

It has protection and is actively using an NHOP backup tunnel at its second hop.

It has no local protection at its third hop.

The RRO display shows the following information for each hop:

Whether local protection is available (that is, whether the LSP has selected a backup tunnel)

Whether local protection is in use (that is, whether the LSP is currently using its selected backup tunnel)

Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel

Whether the backup tunnel used at this hop provides bandwidth protection

---

This section describes the following:

[LSPs Do Not Become Active; They Remain Ready, page 31](#)

[Primary Tunnel Does Not Select Backup Tunnel That Is Up, page 32](#)

[Enhanced RSVP Commands, page 32](#)

[RSVP Hello, page 32](#)

[Hello Instances Have Not Been Created, page 32](#)

[No entry at index \(error may self-correct, RRO may not yet have propagated from downstream node of interest\)" Error Message Is Printed at the Point of Local Repair, page 33](#)

[Couldn't get rsbs \(error may self-correct when Resv arrives\)" Error Message Is Printed at the Point of Local Repair, page 33](#)

### **LSPs Do Not Become Active; They Remain Ready**

-

- 

### Primary Tunnel Does Not Select Backup Tunnel That Is Up

- shutdown
- no shutdown



#### Note

### Enhanced RSVP Commands

- show ip rsvp request
- show ip rsvp reservation
- show ip rsvp sender

show mpls forwarding

### RSVP Hello

### Hello Instances Have Not Been Created

- (configuration) ip rsvp signalling hello
- signalling hello (interface) ip rsvp
- show ip rsvp sender



**No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)" Error Message Is Printed at the Point of Local Repair**

receiving Path messages with the SESSION\_ATTRIBUTE bit indicating that the LSP is fast-reroutable should include an RRO in the corresponding Resv messages.

If an LSP is configured for FRR, but the Resv arriving from a downstream router contains an incomplete RRO, the "No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)" message is printed. An incomplete RRO is one in which the NHOP or the NNHOP did not include an entry in the RRO.

This error typically means that backup tunnels to the NHOP or the NNHOP cannot be selected for this LSP because there is insufficient information about the NHOP or NNHOP due to the lack of an RRO entry.

Occasionally there are valid circumstances in which this situation occurs temporarily and the problem is self-corrected. If subsequent Resv messages arrive with a complete RRO, ignore the error message.

To determine whether the error has been corrected, view the RRO in Resv messages by entering the **clear ip rsvp hello instance counters** command. Use an output filter keyword to view only the LSP of interest.

**Couldn't get rsbs (error may self-correct when Resv arrives)" Error Message Is Printed at the Point of Local Repair**

The PLR cannot select a backup tunnel for an LSP until a Resv message has arrived from downstream.

When this error occurs, it typically means that something is truly wrong. For example, no reservation exists for this LSP. You can troubleshoot this problem by using the **debug ip rsvp reservation** command to enable debug.

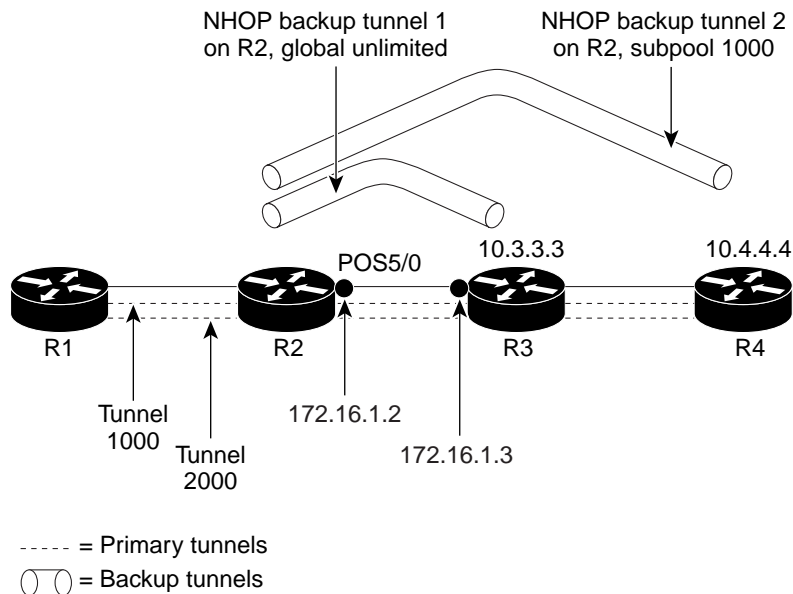
Occasionally there are valid circumstances in which this error message occurs and there is no need for concern. One such circumstance is when an LSP experiences a change before any Resv message has arrived from downstream. Changes can cause a PLR to try to select a backup tunnel for an LSP, and the selection will fail (causing this error message) if no Resv message has arrived for this LSP.

## Configuration Examples for MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

This section provides the following configuration examples:

- [Enabling Fast Reroute for All Tunnels: Example, page 34](#)
- [Creating an NNHOP Backup Tunnel: Example, page 35](#)
- [Assigning Backup Tunnels to a Protected Interface: Example, page 35](#)
- [Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example, page 35](#)
- [Configuring Backup Bandwidth Protection: Example, page 35](#)
- [Configuring an Interface for Fast Link and Node Failure Detection: Example, page 36](#)
- [Configuring an Interface for Fast Tunnel Interface Down: Example, page 36](#)
- [Configuring RSVP Hello and POS Signals: Example, page 36](#)

The examples relate to the illustration shown in [Figure 9](#).

**Figure 9 Backup Tunnels**

59561

## Enabling Fast Reroute for All Tunnels: Example

```

tunnel mpls traffic-eng fast-reroute                                bw-prot    node-prot

Router(config)# interface Tunnel1000
    tunnel mpls traffic-eng fast-reroute
    tunnel mpls traffic-eng bandwidth sub-pool 10

interface Tunnel2000
    tunnel mpls traffic-eng fast-reroute bw-prot node-prot
    tunnel mpls traffic-eng bandwidth 5
  
```

## Creating an NHOP Backup Tunnel: Example

```

ip explicit-path name avoid-protected-link
    exclude-address 10.1.1.2

end

interface Tunnel1
    ip unnumbered loopback0
  
```

```
tunnel destination 10.3.3.3
tunnel mode mpls traffic-eng0
unnel mpls traffic-eng path-option explicit avoid-protected-link
```

## Creating an NNHOP Backup Tunnel: Example

```
ip explicit-path name avoid-protected-node
    exclude-address 10.3.3.3

end

interface Tunnel2
    ip unnumbered loopback0
    tunnel destination 10.4.4.4
    tunnel mode mpls traffic-eng0
    tunnel mpls traffic-eng path-option explicit avoid-protected-node
```

## Assigning Backup Tunnels to a Protected Interface: Example

```
interface POS5/0
    mpls traffic-eng backup-path tunnel1
    mpls traffic-eng backup-path tunnel2
```

## Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example

```
interface Tunnel1
    tunnel mpls traffic-eng backup-bw global-pool Unlimited

interface Tunnel2
    tunnel mpls traffic-eng backup-bw sub-pool 1000
```

## Configuring Backup Bandwidth Protection: Example



### Note

```
tunnel mpls traffic-eng fast-reroute bw-protect
mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

## Configuring an Interface for Fast Link and Node Failure Detection: Example

```
interface pos0/0
 pos ais-shut
```

```
interface pos0/0
 pos report lrld
```

## Configuring an Interface for Fast Tunnel Interface Down: Example

```
interface tunnel 1000
 tunnel mpls traffic-eng interface down delay 0
```

## Configuring RSVP Hello and POS Signals: Example

- ip rsvp signalling hello
- ip rsvp signalling hello
- ip rsvp signalling hello dscp
- ip rsvp signalling hello refresh misses
- ip rsvp signalling hello refresh interval
- ip rsvp signalling hello statistics

*MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support*

```
pos ais-shut
pos report rdool
pos report lais
pos report lrld
pos report pais
pos report prdi
pos report sd-ber
```

# Additional References

## Related Documents

| Related Topic | Document Title                                                                                                                                                                     |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <a href="#">MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</a>                                                            |
|               | <ul style="list-style-type: none"> <li><a href="#">MPLS Traffic Engineering: Shared Risk Link Groups</a></li> <li><a href="#">MPLS Traffic Engineering: Inter-AS TE</a></li> </ul> |
|               | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                                                                          |
|               | <a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>                                                                                                           |

## Standards

| Standards | Title |
|-----------|-------|
|           |       |

## MIBs

| MIBs | MIBs Link |
|------|-----------|
|      |           |

## RFCs

| RFCs | Title                                                              |
|------|--------------------------------------------------------------------|
|      | <a href="#">Fast Reroute Extensions to RSVP-TE for LSP Tunnels</a> |

# Technical Assistance

| Description | Link |
|-------------|------|
|             |      |

# Command Reference

Command Reference

Cisco IOS Multiprotocol Label Switching

-



**Table 3**      **Feature Information for MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) (continued)**

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>• Link protection for GE interfaces on 10x1G engine 4+ GE, 1x10G engine 4+ GE, and 4x1G engine 3 GE routers with the Loss of Signal Fast Reroute trigger</li><li>• The <code>mpls te link-protection</code> command was added.</li></ul> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p> |



# Glossary

—The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

—An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

—The available traffic capacity of a link.

**Cisco Express Forwarding**

**enterprise network**

**Fast Reroute**

**Gigabit Ethernet**

**global pool**

**headend**

**hop**

**instance**

**interface**

**Intermediate System-to-Intermediate System**

**link**

**limited backup bandwidth**

**load balancing**

**LSP**

**merge point**

**MPLS**

**MPLS global label allocation**

**NHOP**

**NHOP backup tunnel**

**NNHOP**

**NNHOP backup tunnel**

**node**

**OSPF**

**primary LSP**

**primary tunnel**

**promotion**

**protected interface**

**redundancy**

**RSVP**

**scalability**

**state**

**subpool**

**tailend**

**topology**

**tunnel**

**unlimited backup bandwidth**

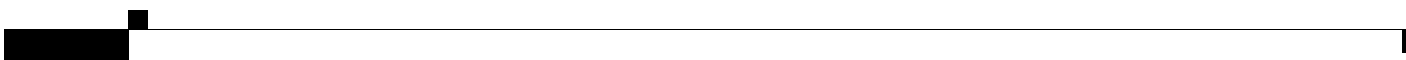
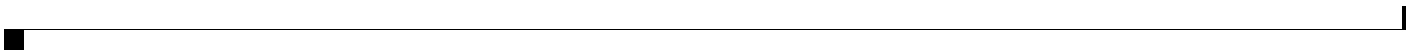
CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers,

Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.





# MPLS Traffic Engineering: BFD-triggered Fast Reroute

---

**First Published:** January 8, 2008

**Last Updated:** February 18, 2009

The MPLS Traffic Engineering: BFD-triggered Fast Reroute feature allows you to obtain link and node protection by using the Bidirectional Forwarding Detection (BFD) protocol to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators.

To obtain link and node protection by using the Resource Reservation Protocol (RSVP) with Hellos support, refer to the [MPLS TE: Link and Node Protection, with RSVP Hellos Support \(with Fast Tunnel Interface Down Detection\)](#) process module. RSVP Hellos enable a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering: BFD-triggered Fast Reroute”](#) section on page 25.

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

## Contents

- [Prerequisites for MPLS Traffic Engineering: BFD-triggered Fast Reroute, page 2](#)
- [Restrictions for MPLS Traffic Engineering: BFD-triggered Fast Reroute, page 2](#)
- [Information About MPLS Traffic Engineering: BFD-triggered Fast Reroute, page 2](#)



---

**Americas Headquarters:**

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

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

- [How to Configure MPLS Traffic Engineering: BFD-triggered Fast Reroute](#), page 4
- [Configuration Examples for MPLS Traffic Engineering: BFD-triggered Fast Reroute](#), page 19
- [Additional References](#), page 22
- [Command Reference](#), page 24
- [Feature Information for MPLS Traffic Engineering: BFD-triggered Fast Reroute](#), page 25
- [Glossary](#), page 26

## Prerequisites for MPLS Traffic Engineering: BFD-triggered Fast Reroute

- Configure BFD. Refer to the *Bidirectional Forwarding Detection* process module.
- Enable MPLS TE on all relevant routers and interfaces.
- Configure MPLS TE tunnels.
- For additional prerequisites, refer to the *MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)* process module.

## Restrictions for MPLS Traffic Engineering: BFD-triggered Fast Reroute

- You cannot configure BFD and RSVP Hellos on the same interface.
- BFD may not be supported on some interfaces.
- For additional restrictions, refer to the *MPLS TE: Link and Node protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)* process module.

## Information About MPLS Traffic Engineering: BFD-triggered Fast Reroute

To configure the MPLS Traffic Engineering: BFD-triggered Fast Reroute feature, you need to understand the following concepts:

- [BFD](#), page 3
- [Fast Reroute](#), page 3
- [Link Protection](#), page 3
- [Node Protection](#), page 3
- [Bandwidth Protection](#), page 3

## BFD

BFD is a detection protocol designed to provide fast forwarding path failure detection times for all media types, encapsulations, topologies, and routing protocols. In addition to fast forwarding path failure detection, BFD provides a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol Hello mechanisms, network profiling and planning will be easier, and reconvergence time will be consistent and predictable.

## Fast Reroute

Fast Reroute (FRR) is a mechanism for protecting Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switched paths (LSPs) from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

## Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure.

## Node Protection

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link as well as the node.

## Bandwidth Protection

NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected.

# How to Configure MPLS Traffic Engineering: BFD-triggered Fast Reroute

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured.

To review how to configure MPLS TE tunnels, see the [MPLS Traffic Engineering: Interarea Tunnels](#) process module.

The following sections describe how to use FRR to protect LSPs in your network from link or node failures. Each task is identified as either required or optional.

**Note**

You can perform the configuration tasks in any order.

**Note**

An NNHOP backup tunnel must *not* go via the NHOP backup tunnel.

- [Enabling BFD Support on the Router, page 4](#) (required)
- [Enabling Fast Reroute on LSPs, page 5](#) (required)
- [Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop, page 6](#) (required)
- [Assigning Backup Tunnels to a Protected Interface, page 8](#) (required)
- [Enabling BFD on the Protected Interface, page 10](#) (required)
- [Associating Backup Bandwidth and Pool Type with a Backup Tunnel, page 10](#) (optional)
- [Configuring Backup Bandwidth Protection, page 11](#) (optional)
- [Verifying That Fast Reroute Is Operational, page 12](#) (optional)

## Enabling BFD Support on the Router

To enable support for Bidirectional Forwarding on the router, enter the following commands.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello bfd**



## DETAILED STEPS

|        | Command                                                                                                    | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                             | Enters global configuration mode.                                                                                |
| Step 3 | <b>ip rsvp signalling hello bfd</b><br><br><b>Example:</b><br>Router(config)# ip rsvp signalling hello bfd | Enables the BFD protocol on the router for MPLS TE link and node protection.                                     |

## Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if the LSPs have been configured as fast reroutable. To enable FRR on the LSP, enter the following commands at the headend of each LSP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng fast-reroute [bw-protect] [node-protect]**

## DETAILED STEPS

|        | Command                                                                        | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command                                                                                                         | Purpose                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Step 3 | <code>interface tunnel <i>number</i></code>                                                                     | Enters interface configuration mode for the specified tunnel.                                     |
|        | <b>Example:</b><br><code>Router(config)# interface tunnel 1000</code>                                           |                                                                                                   |
| Step 4 | <code>tunnel mpls traffic-eng fast-reroute [bw-protect] [node-protect]</code>                                   | Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure. |
|        | <b>Example:</b><br><code>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect</code> |                                                                                                   |

## Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop

To create a backup tunnel to the next hop or to the next-next hop, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the [“Finding Feature Information”](#) section on page 1.

Creating a backup tunnel is basically no different from creating any other tunnel.



### Note

When using the **exclude-address** command to specify the path for a backup tunnel, you must exclude an interface address to avoid a link (for creating an NHOP backup tunnel), or a router-ID address to avoid a node (for creating an NNHOP backup tunnel).

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `ip unnumbered type number`
5. `tunnel destination A.B.C.D`
6. `tunnel mode mpls traffic-eng`
7. `tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name | path-number}} [lockdown]`
8. `exit`
9. `ip explicit-path name name`
10. `exclude-address address`

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                         | Enters global configuration mode.                                                                                                                                                                    |
| Step 3 | <b>interface tunnel number</b><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                                                                                                                            | Creates a new tunnel interface and enters interface configuration mode.                                                                                                                              |
| Step 4 | <b>ip unnumbered type number</b><br><br><b>Example:</b><br>Router(config-if)# ip unnumbered loopback 0                                                                                                                                 | Gives the tunnel interface an IP address that is the same as that of interface loopback 0.<br><br><b>Note</b> This command is not effective until loopback 0 has been configured with an IP address. |
| Step 5 | <b>tunnel destination A.B.C.D</b><br><br><b>Example:</b><br>Router(config-if)# tunnel destination 10.3.3.3                                                                                                                             | Specifies the IP address of the device where the tunnel will terminate. That address should be the router ID of the device that is the NHOP or NNHOP of LSPs to be protected.                        |
| Step 6 | <b>tunnel mode mpls traffic-eng</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mode mpls traffic-eng                                                                                                                          | Sets encapsulation mode of the tunnel to MPLS TE.                                                                                                                                                    |
| Step 7 | <b>tunnel mpls traffic-eng path-option number {dynamic   explicit {name path-name   path-number}}[lockdown]</b><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit name avoid-protected-link | Configures a path option for an MPLS TE tunnel                                                                                                                                                       |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                                                          | Exits interface configuration mode.                                                                                                                                                                  |

|         | Command                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <code>ip explicit-path name <i>name</i></code><br><br><b>Example:</b><br>Router(config)# ip explicit-path name<br>avoid-protected-link | Enters IP explicit path mode for IP explicit paths to create the named path.                                                                                                                                                                                                                                                                                                       |
| Step 10 | <code>exclude-address <i>address</i></code><br><br><b>Example:</b><br>Router(cfg-ip-expl-path)# exclude-address 10.3.3.3               | For link protection, specifies the IP address of the link to be protected. For node protection, specifies the router ID of the node to be protected.<br><br><b>Note</b> Backup tunnel paths can be dynamic or explicit and they do not have to use an excluded address. Because backup tunnels must avoid the protected link or node, it is convenient to use an excluded address. |

## Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the [“Finding Feature Information”](#) section on page 1.



### Note

You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `mpls traffic-eng backup-path tunnel tunnel-id`

## DETAILED STEPS

|        | Command                                                                              | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                     |

|        | Command                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface Gi 9/1                                             | Moves configuration to the physical interface level, directing subsequent configuration commands to the specific physical interface identified by the <i>type</i> value, and enters interface configuration mode. The <i>slot</i> and <i>port</i> values identify the slot and port being configured. The interface must be a supported interface. See the <a href="#">“Finding Feature Information” section on page 1</a> . |
| Step 4 | <b>mpls traffic-eng backup-path tunnel</b> <i>tunnel-id</i><br><br><b>Example:</b><br>Router(config-if)# mpls traffic-eng backup-path tunnel2 | Allows LSPs going out this interface to use this backup tunnel if there is a link or node failure.<br><br><b>Note</b> You can enter this command multiple times to associate multiple backup tunnels with the same protected interface.                                                                                                                                                                                      |

# Enabling BFD on the Protected Interface

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp signalling hello bfd**
5. **bfd interval** *milliseconds* **min\_rx** *milliseconds* **multiplier** *interval-multiplier*

## DETAILED STEPS

|        | Command                                                                                                                                                                                                      | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                               | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Gi9/1                                                                                                                | Enters interface configuration mode.                                                                             |
| Step 4 | <b>ip rsvp signalling hello bfd</b><br><br><b>Example:</b><br>Router(config-if)# ip rsvp signalling hello bfd                                                                                                | Enables the BFD protocol on the interface for MPLS TE link and node protection.                                  |
| Step 5 | <b>bfd interval</b> <i>milliseconds</i> <b>min_rx</b> <i>milliseconds</i> <b>multiplier</b> <i>interval-multiplier</i><br><br><b>Example:</b><br>Router(config-if)# bfd interval 100 min_rx 100 multiplier 4 | Sets the BFD interval.                                                                                           |

# Associating Backup Bandwidth and Pool Type with a Backup Tunnel

To associate backup bandwidth with a backup tunnel and designate the type of LSP that can use a backup tunnel, enter the following commands.

## SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng backup-bw** {*bandwidth* | [**sub-pool** {*bandwidth* | **Unlimited**}] [**global-pool** {*bandwidth* | **Unlimited**}] [**any** {*bandwidth* | **Unlimited**}]

## DETAILED STEPS

|        | Command                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                            | Enters global configuration mode.                                                                                                         |
| Step 3 | <b>interface tunnel</b> <i>number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 2                                                                                                                                                                                                                                        | Enters interface configuration mode for the specified tunnel.                                                                             |
| Step 4 | <b>tunnel mpls traffic-eng backup-bw</b> { <i>bandwidth</i>   [ <b>sub-pool</b> { <i>bandwidth</i>   <b>Unlimited</b> }] [ <b>global-pool</b> { <i>bandwidth</i>   <b>Unlimited</b> }] [ <b>any</b> { <i>bandwidth</i>   <b>Unlimited</b> }]<br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000 | Associates bandwidth with a backup tunnel and designates whether LSPs that allocate bandwidth from the specified pool can use the tunnel. |

## Configuring Backup Bandwidth Protection

To configure the backup bandwidth protection, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng fast-reroute** [bw-protect]
5. **exit**
6. **mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw**

## DETAILED STEPS

|        |                                                                                                                                                                                          |                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                              |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal                                                                                                     | Enters global configuration mode.                                                                                                                                                                             |
| Step 3 | <code>interface tunnel number</code><br><br><b>Example:</b><br>Router(config)# interface tunnel 2                                                                                        | Enters interface configuration mode for the specified tunnel.                                                                                                                                                 |
| Step 4 | <code>tunnel mpls traffic-eng fast-reroute [bw-protect]</code><br><br><b>Example:</b><br>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect                              | Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure. The <b>bw-protect</b> keyword gives an LSP priority for using backup tunnels with bandwidth protection. |
| Step 5 | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                      | Exits interface configuration mode.                                                                                                                                                                           |
| Step 6 | <code>mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw</code><br><br><b>Example:</b><br>Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw | Changes the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.                                                      |

## Verifying That Fast Reroute Is Operational

To verify that FRR can function, perform the following steps.

## SUMMARY STEPS



## Note

To determine if FRR has been configured correctly, perform Steps 1 and 2.



## Note

If you created LSPs and performed the required configuration tasks but do not have operational backup tunnels (that is, the backup tunnels are not up or the LSPs are not associated with those backup tunnels), perform Step 3.



**Note**

To determine the status of BFD, perform Steps 9 through 11.

1. **show mpls traffic-eng tunnels brief**
2. **show ip rsvp sender detail**
3. **show mpls traffic-eng fast-reroute database**
4. **show mpls traffic-eng tunnels backup**
5. **show mpls traffic-eng fast-reroute database**
6. **show ip rsvp reservation**
7. **show ip rsvp hello**
8. **show ip rsvp interface detail**
9. **show ip rsvp hello bfd nbr**
10. **show ip rsvp hello bfd nbr detail**
11. **show ip rsvp hello bfd nbr summary**

**DETAILED STEPS****Step 1 show mpls traffic-eng tunnels brief**

Use this command to verify that backup tunnels are up:

```
Router# show mpls traffic-eng tunnels brief
```

```

Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:            running
  Forwarding:              enabled
  Periodic reoptimization:  every 3600 seconds, next in 1706 seconds

TUNNEL NAME      DESTINATION    UP IF    DOWN IF    STATE/PROT
Router_t1        10.112.0.12    -        Gi4/0/1    up/up
Router_t2        10.112.0.12    -        unknown    up/down
Router_t3        10.112.0.12    -        unknown    admin-down
Router_t1000     10.110.0.10    -        unknown    up/down
Router_t2000     10.110.0.10    -        Gi4/0/1    up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails

```

**Step 2 show ip rsvp sender detail**

Use this command to verify that LSPs are protected by the appropriate backup tunnels.

Following is sample output from the **show ip rsvp sender detail** command when the command is entered at the router acting as the point of local repair (PLR) before a failure:

```
Router# show ip rsvp sender detail
```

```

PATH:
Tun Dest:  10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1  LSP ID: 31
Path refreshes:
  arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: (0x7) Local Prot desired, Label Recording, SE Style
  session Name: Rl_t100
  ERO: (incoming)

```

```

10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
  10.10.7.1/32, Flags:0x0 (No Local Protection)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
  10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated

```

### Step 3 show mpls traffic-eng fast-reroute database

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR Node Protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

Router# **show mpls traffic-eng fast-reroute database**

Tunnel head end item frr information:

| Protected tunnel | In-label | Out intf/label   | FRR intf/label | Status |
|------------------|----------|------------------|----------------|--------|
| Tunnel500        | Tun hd   | AT4/0.100:Untagg | Tu501:20       | ready  |

Prefix item frr information:

| Prefix      | Tunnel | In-label | Out intf/label   | FRR intf/label | Status |
|-------------|--------|----------|------------------|----------------|--------|
| 10.0.0.8/32 | Tu500  | 18       | AT4/0.100:Pop ta | Tu501:20       | ready  |
| 10.0.8.8/32 | Tu500  | 19       | AT4/0.100:Untagg | Tu501:20       | ready  |
| 10.8.9.0/24 | Tu500  | 22       | AT4/0.100:Untagg | Tu501:20       | ready  |

LSP midpoint item frr information:

| LSP identifier | In-label | Out | intf/label | FRR intf/label | Status |
|----------------|----------|-----|------------|----------------|--------|
|----------------|----------|-----|------------|----------------|--------|

If Label Distribution Protocol (LDP) is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table ip-address detail** command. The final line of the display will tell whether that prefix is protected:

Router# **show mpls forwarding-table 10.0.0.11 32 detail**

| Local tag                                               | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|---------------------------------------------------------|--------------------|---------------------|--------------------|--------------------|-------------|
| Tun hd                                                  | Untagged           | 10.0.0.11/32        | 48 5/0             | Gi5/0              | point2point |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22}                 |                    |                     |                    |                    |             |
| 48D18847 00016000                                       |                    |                     |                    |                    |             |
| No output feature configured                            |                    |                     |                    |                    |             |
| Fast Reroute Protection via (Tu0, outgoing label 12304) |                    |                     |                    |                    |             |

The following command output displays the LSPs that are protected when the FRR primary tunnel is over a Gigabit Ethernet interface and the backup tunnel is over a Gigabit Ethernet interface. As shown in [Figure 1](#), interface Gigabit Ethernet 9/1 is protected by backup tunnel 501.

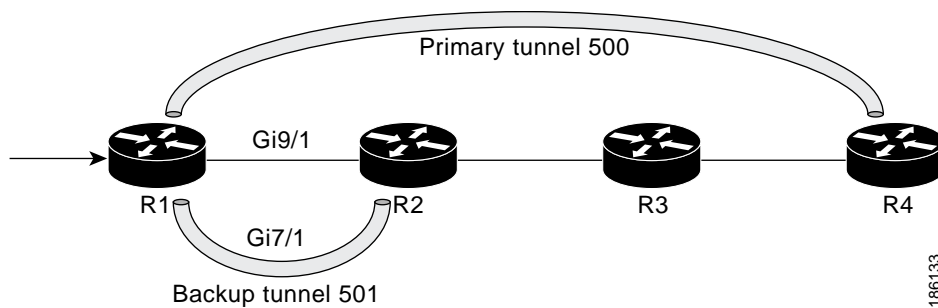
**Figure 1**      **Protected LSPs**

Figure 1 shows the following:

- Primary tunnel 500—Path is R1 via Gigabit Ethernet9/1 to R2 to R3 to R4.
- FRR backup tunnel 501—Path is R1 via Gigabit Ethernet7/1 to R2.
- Interface Gigabit Ethernet9/1—Protected by backup tunnel 501.

```
Router# show mpls traffic-eng fast-reroute database
```

```
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd AT4/0.100:Untagg Tu501:20 ready
Prefix item frr information:
```

```
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 AT4/0.100:Pop ta Tu501:20 ready
10.0.8.8/32 Tu500 19 AT4/0.100:Untagg Tu501:20 ready
10.8.9.0/24 Tu500 22 AT4/0.100:Untagg Tu501:20 ready
```

```
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

The following command output displays the LSPs that are protected when the FRR backup tunnel is over a Gigabit Ethernet interface.

```
Router# show mpls traffic-eng fast-reroute database
```

```
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd PO2/0:Untagged Tu501:20 ready
```

```
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 PO2/0:Pop tag Tu501:20 ready
10.0.8.8/32 Tu500 19 PO2/0:Untagged Tu501:20 ready
10.8.9.0/24 Tu500 22 PO2/0:Untagged Tu501:20 ready
```

```
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

#### Step 4 **show mpls traffic-eng tunnels backup**

For backup tunnels to be operational, the LSP must be reroutable. At the headend of the LSP, enter the **show run interface tunnel *tunnel-number*** command. The output should include the **tunnel mpls traffic-eng fast-reroute** command. If it does not, enter this command for the tunnel.

On the router where the backup tunnels originate, enter the **show mpls traffic-eng tunnels backup** command. Following is sample command output:

```
Router# show mpls traffic-eng tunnels backup

Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0, PO1/1, PO3/3
    Protected lsp: 1
    Backup BW: any pool unlimited; inuse: 100 kbps

Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1
    Protected lsp: 0
    Backup BW: any pool unlimited; inuse: 0 kbps

Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0
    Protected lsp: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The command output will allow you to verify the following:

- Backup tunnel exists—Verify that there is a backup tunnel that terminates at this LSP’s NHOP or NNHOP. Look for the LSP’s NHOP or NNHOP in the Dest field.
- Backup tunnel is up—To verify that the backup tunnel is up, look for “Up” in the Oper field.
- Backup tunnel is associated with the LSP’s interface—Verify that the interface for the LSP is allowed to use this backup tunnel. Look for the LSP’s output interface in the protected i/fs field list.
- Backup tunnel has sufficient bandwidth—If you restricted the amount of bandwidth a backup tunnel can hold, verify that the backup tunnel has sufficient bandwidth to hold the LSPs that would use this backup tunnel if there is a failure. The bandwidth of an LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of the LSP. To determine the available bandwidth on a backup tunnel, look at the “cfg” and “inuse” fields. If there is insufficient backup bandwidth to accommodate the LSPs that would use this backup tunnel in the event of a failure, create an additional backup tunnel or increase the backup bandwidth of the existing tunnel by using the **tunnel mpls traffic-eng bandwidth** command.



#### Note

In order to determine how much bandwidth is sufficient, offline capacity planning may be required.

Backup tunnel has appropriate bandwidth type—If you restricted the type of LSPs (subpool or global pool) that can use this backup tunnel, verify that the LSP is the appropriate type for the backup tunnel. The type of the LSP is defined by the line **tunnel mpls traffic-eng bandwidth** at the headend of this LSP. If this line contains the word “sub pool”, then it uses subpool bandwidth; otherwise, it uses global pool bandwidth. Verify that the type matches the type the backup tunnel can hold by looking in the output of the **tunnel mpls traffic-eng bandwidth** command.

If none of the verification actions described succeed, enable debug by entering the **debug ip rsvp fast-reroute** command and the **debug mpls traffic-eng fast-reroute** command on the router that is the headend of the backup tunnel. Then do the following:

1. Enter the **shutdown** command for the primary tunnel.

2. Enter the **no shutdown** command for the primary tunnel.
3. View the debug output.

#### Step 5 show mpls traffic-eng fast-reroute database

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR node protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

```
Router# show mpls traffic-eng fast-reroute database
```

Tunnel head end item frr information:

| Protected Tunnel | In-label | intf/label     | FRR intf/label | Status |
|------------------|----------|----------------|----------------|--------|
| Tunnell0         | Tun      | Gi5/0:Untagged | Tu0:12304      | ready  |

Prefix item frr information:

| Prefix       | Tunnel | In-label | Out intf/label | FRR intf/label | Status |
|--------------|--------|----------|----------------|----------------|--------|
| 10.0.0.11/32 | Tu10   | Tun hd   | Gi5/0:Untagged | Tu0:12304      | ready  |

LSP midpoint frr information:

| LSP identifier    | In-label | Out intf/label | FRR intf/label | Status |
|-------------------|----------|----------------|----------------|--------|
| 10.0.0.12 1 [459] | 16       | Gi0/1:17       | Tu2000:19      | ready  |



#### Note

If Label Distribution Protocol (LDP) is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table ip-address detail** command. The final line of the display will tell whether that prefix is protected.

```
Router# show mpls forwarding-table 10.0.0.11 32 detail
```

| Local                                                   | Outgoing  | Prefix       | Bytes tag | Outgoing    | Next Hop |
|---------------------------------------------------------|-----------|--------------|-----------|-------------|----------|
| tag                                                     | tag or VC | or Tunnel Id | switched  | interface   |          |
| Tun hd                                                  | Untagged  | 10.0.0.11/32 | 48 Gi5/0  | point2point |          |
| MAC/Encaps=4/8, MTU=1520, Tag Stack{22}                 |           |              |           |             |          |
| 48D18847 00016000                                       |           |              |           |             |          |
| No output feature configured                            |           |              |           |             |          |
| Fast Reroute Protection via (Tu0, outgoing label 12304) |           |              |           |             |          |

#### Step 6 show ip rsvp reservation detail

Following is sample output from the **show ip rsvp reservation detail** command entered at the headend of a primary LSP. Entering the command at the headend of the primary LSP shows, among other things, the status of FRR (that is, local protection) at each hop this LSP traverses. The per-hop information is collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

```
Router# show ip rsvp reservation detail
```

Reservation:

Tun Dest: 10.1.1.1 Tun ID: 1 Ext Tun ID: 10.1.1.1

Tun Sender: 10.1.1.1 LSP ID: 104

Next Hop: 10.1.1.2 on Gi1/0

Label: 18 (outgoing)

Reservation Style is Shared-Explicit, QoS Service is Controlled-Load

Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes

Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes

RRO:

10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)

```

    Label subobject: Flags 0x1, C-Type 1, Label 18
10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 16
10.1.1.2/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 0
Resv ID handle: CD000404.
Policy: Accepted. Policy source(s): MPLS/TE

```

Notice the following about the primary LSP:

- It has protection that uses an NHOP backup tunnel at its first hop.
- It has protection and is actively using an NHOP backup tunnel at its second hop.
- It has no local protection at its third hop.

The RRO display shows the following information for each hop:

- Whether local protection is available (that is, whether the LSP has selected a backup tunnel)
- Whether local protection is in use (that is, whether the LSP is using its selected backup tunnel)
- Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel
- Whether the backup tunnel used at this hop provides bandwidth protection

#### Step 7 show ip rsvp hello

Use this command to display hello status and statistics for FRR, reroute (hello state timer), and graceful restart. Following is sample output:

```

Router# show ip rsvp hello

Hello:
  RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
  BFD for Fast-Reroute/Reroute: Enabled
  RSVP Hello for Graceful Restart: Disabled

```

#### Step 8 show ip rsvp interface detail

Use this command to display the interface configuration for Hello. Following is sample output:

```

Router# show ip rsv interface detail

Gi9/47:
  RSVP: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 0 bits/sec
    Max. allowed (per flow): 0 bits/sec
    Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs: 0x3F
    Number of refresh intervals to enforce blockade state: 4
  Authentication: disabled
  Key chain: <none>
  Type: md5
  Window size: 1
  Challenge: disabled
  FRR Extension:
    Backup Path: Configured (or "Not Configured")
  BFD Extension:
    State: Disabled

```

```
Interval: Not Configured
RSVP Hello Extension:
State: Disabled
Refresh Interval: FRR: 200 , Reroute: 2000
Missed Acks:      FRR: 4 , Reroute: 4
DSCP in HELLOs:   FRR: 0x30 , Reroute: 0x30
```

**Step 9 show ip rsvp hello bfd nbr**

Use this command to display information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol. Following is sample output. The command output is the same as the **show ip rsvp hello bfd nbr summary** command output.

```
Router# show ip rsvp hello bfd nbr
```

| Client | Neighbor | I/F    | State | LostCnt | LSPs |
|--------|----------|--------|-------|---------|------|
| FRR    | 10.0.0.6 | Gi9/47 | Up    | 0       | 1    |

**Step 10 show ip rsvp hello bfd nbr detail**

Use this command to display detailed information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol:

```
Router# show ip rsvp hello bfd nbr detail
```

```
Hello Client Neighbors
```

```
Remote addr 10.0.0.6, Local addr 10.0.0.7
Type: Active
I/F: Gi9/47
State: Up (for 00:09:41)
Clients: FRR
LSPs protecting: 1 (frr: 1, hst upstream: 0 hst downstream: 0)
Communication with neighbor lost: 0
```

**Step 11 show ip rsvp hello bfd nbr summary**

Use this command to display summarized information about all MPLS traffic engineering link and node protected neighbors that use the BFD protocol. The command output is the same as the **show ip rsvp hello bfd nbr summary** command output.

```
Router# show ip rsvp hello bfd nbr summary
```

| Client | Neighbor | I/F    | State | LostCnt | LSPs |
|--------|----------|--------|-------|---------|------|
| FRR    | 10.0.0.6 | Gi9/47 | Up    | 0       | 1    |

## Configuration Examples for MPLS Traffic Engineering: BFD-triggered Fast Reroute

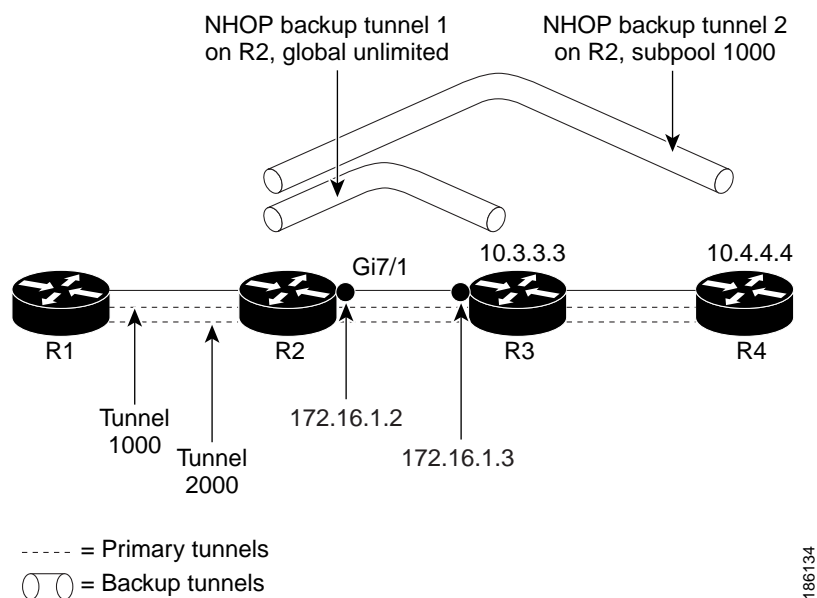
This section provides the following configuration examples:

- [Enabling BFD Support on the Router: Example, page 20](#)
- [Enabling Fast Reroute on LSPs: Example, page 20](#)
- [Creating a Backup Tunnel to the Next Hop: Example, page 21](#)
- [Assigning Backup Tunnels to a Protected Interface: Example, page 21](#)

- [Enabling BFD on the Protected Interface: Example, page 21](#)
- [Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example, page 21](#)
- [Configuring Backup Bandwidth Protection: Example, page 22](#)

The examples relate to the illustration shown in [Figure 2](#).

**Figure 2 Backup Tunnels**



## Enabling BFD Support on the Router: Example

The following example enables the BFD protocol on the router:

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

## Enabling Fast Reroute on LSPs: Example

On router R1, enter interface configuration mode for each tunnel to be protected (Tunnel 1000 and Tunnel 2000). Enable these tunnels to use a backup tunnel in case of a link or node failure along their paths.

Tunnel 1000 will use ten units of bandwidth from the subpool.

Tunnel 2000 will use five units of bandwidth from the global pool. The “bandwidth protection desired” bit and the “node protection desired bit” have been set by specifying **bw-prot** and **node-prot**, respectively, in the **tunnel mpls traffic-eng fast-reroute** command.

```
Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
```

```
Router(config)# interface tunnel 2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect node-protect
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```



## Creating a Backup Tunnel to the Next Hop: Example

On router R2, create an NHOP backup tunnel to R3. This backup tunnel should avoid using the link 10.1.1.2.

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 10.1.1.2
Explicit Path name avoid-protected-link:
____1: exclude-address 10.1.1.2
Router(cfg-ip-expl-path)# end

Router(config)# interface tunnel 1
Router(config-if)# ip unnumbered loopback 0
Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit avoid-protected-link
```

## Creating an NNHOP Backup Tunnel: Example

On router R2, create an NNHOP backup tunnel to R4. This backup tunnel should avoid R3.

```
Router(config)# ip explicit-path name avoid-protected-node
Router(cfg-ip-expl-path)# exclude-address 10.3.3.3
Explicit Path name avoid-protected-node:
____1: exclude-address 10.3.3.3
Router(cfg-ip-expl-path)# end

Router(config)# interface tunnel2
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.4.4.4
Router(config-if)# tunnel mode mpls traffic-eng0
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit avoid-protected-node
```

## Assigning Backup Tunnels to a Protected Interface: Example

On router R2, associate both backup tunnels with interface Gigabit Ethernet 5/0:

```
Router(config)# interface Gi5/0
Router(config-if)# mpls traffic-eng backup-path tunnel 1
Router(config-if)# mpls traffic-eng backup-path tunnel 2
```

## Enabling BFD on the Protected Interface: Example

BFD is enabled on interface Gigabit Ethernet 9/47:

```
Router(config)# interface Gi9/47
Router(config-if)# ip rsvp signalling hello bfd
Router(config-if)# bfd interval 100 min_rx 100 multiplier 4
```

## Associating Backup Bandwidth and Pool Type with Backup Tunnels: Example

Backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. It does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface tunnel 1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited

Router(config)# interface tunnel 2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```

## Configuring Backup Bandwidth Protection: Example

In the following example, backup bandwidth protection is configured:

**Note**

---

This global configuration is required only to change the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

---

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering: BFD-triggered Fast Reroute feature.

## Related Documents

| Related Topic                                                        | Document Title                                                                                                                 |
|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Link and node protection                                             | <a href="#"><i>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</i></a> |
| Multiprotocol Label Switching commands                               | <a href="#"><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></a>                                               |
| Bidirectional Forwarding Direction configuration information         | <a href="#"><i>Bidirectional Forwarding Detection</i></a>                                                                      |
| MPLS Traffic Engineering Interarea Tunnels configuration information | <a href="#"><i>MPLS Traffic Engineering: Interarea Tunnels</i></a>                                                             |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- **clear ip rsvp hello bfd**
- **ip rsvp signalling hello bfd** (configuration)
- **ip rsvp signalling hello bfd** (interface)
- **show ip rsvp hello**
- **show ip rsvp hello bfd nbr**
- **show ip rsvp hello bfd nbr detail**
- **show ip rsvp hello bfd nbr summary**
- **show ip rsvp interface detail**

# Feature Information for MPLS Traffic Engineering: BFD-triggered Fast Reroute

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Traffic Engineering: BFD-triggered Fast Reroute

| Feature Name                                         | Releases                                   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Traffic Engineering: BFD-triggered Fast Reroute | 12.2(33)SRC<br>Cisco IOS XE<br>Release 2.3 | <p>MPLS Traffic Engineering: BFD-triggered Fast Reroute allows you to obtain link and node protection by using the BFD protocol.</p> <p>In 12.2(33)SRC, this feature was introduced.</p> <p>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 series routers.</p> <p>The following commands were introduced or modified by this feature: <b>clear ip rsvp hello bfd</b>, <b>ip rsvp signalling hello bfd</b> (configuration), <b>ip rsvp signalling hello bfd</b> (interface), <b>show ip rsvp hello</b>, <b>show ip rsvp hello bfd nbr</b>, <b>show ip rsvp hello bfd nbr detail</b>, <b>show ip rsvp hello bfd nbr summary</b>, and <b>show ip rsvp interface detail</b>.</p> |

# Glossary

**backup bandwidth**—The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

**backup tunnel**—An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

**bandwidth**—The available traffic capacity of a link.

**fast reroute**—Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

**global pool**—The total bandwidth allocated to an MPLS traffic engineering link or node.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hop**—Passage of a data packet between two network nodes (for example, between two routers).

**instance**—A Hello instance implements the RSVP Hello extensions for a given router interface address and remote IP address. Active Hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected Ack message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**interface**—A network connection.

**link**—A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**LSP**—label-switched path. A configured connection between two routers, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**NHOP**—next hop. The next downstream node along an LSP's path.

**NHOP backup tunnel**—next-hop backup tunnel. Backup tunnel terminating at the LSP's next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

**NNHOP**—next-next hop. The node after the next downstream node along an LSP's path.

**NNHOP backup tunnel**—next-next-hop backup tunnel. Backup tunnel terminating at the LSP's next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.

**node**—Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Computers on a network, or any endpoint or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations.

**primary LSP**—The last LSP originally signaled over the protected interface before the failure. The LSP before the failure.

**primary tunnel**—Tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**protected interface**—An interface that has one or more backup tunnels associated with it.

**redundancy**—The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

**RSVP**—Resource Reservation Protocol. An IETF protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

**state**—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**subpool**—The more restrictive bandwidth in an MPLS traffic engineering link or node. The subpool is a portion of the link or node's overall global pool bandwidth.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**tunnel**—Secure communications path between two peers, such as two routers.

**unlimited backup bandwidth**—Backup tunnels that provide no bandwidth (best-effort) protection (that is, they provide best-effort protection).

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

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







## **MPLS Layer 2 VPNs**





# Any Transport over MPLS

---

**First Published: January 1, 2001**

**Last Updated: November 20, 2009**

This document describes the Any Transport over MPLS (AToM) feature, which provides the following capabilities:

- Transport data link layer (Layer2) packets over a Multiprotocol Label Switching (MPLS) backbone.
- Enable service providers to connect customer sites with existing Layer 2 networks by using a single, integrated, packet-based network infrastructure—a Cisco MPLS network. Instead of using separate networks with network management environments, service providers can deliver Layer 2 connections over an MPLS backbone.
- Provide a common framework to encapsulate and transport supported Layer 2 traffic types over an MPLS network core.

AToM supports the following like-to-like transport types:

- ATM Adaptation Layer Type-5 (AAL5) over MPLS
- ATM Cell Relay over MPLS
- Ethernet over MPLS (VLAN and port modes)
- Frame Relay over MPLS
- PPP over MPLS
- High-Level Data Link Control (HDLC) over MPLS

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Any Transport over MPLS” section on page 88](#).

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for Any Transport over MPLS, page 2](#)
- [Restrictions for Any Transport over MPLS, page 3](#)
- [Information About Any Transport over MPLS, page 5](#)
- [How to Configure Any Transport over MPLS, page 14](#)
- [Configuration Examples for Any Transport over MPLS, page 67](#)
- [Additional References, page 85](#)
- [Feature Information for Any Transport over MPLS, page 88](#)

## Prerequisites for Any Transport over MPLS

Before configuring AToM, ensure that the network is configured as follows:

- Configure IP routing in the core so that the provider edge (PE) routers can reach each other via IP.
- Configure MPLS in the core so that a label-switched path (LSP) exists between the PE routers.
- Enable Cisco Express Forwarding or distributed Cisco Express Forwarding before configuring any Layer 2 circuits.
- Configure a loopback interface for originating and terminating Layer 2 traffic. Make sure the PE routers can access the other router's loopback interface. Note that the loopback interface is not needed in all cases. For example, tunnel selection does not need a loopback interface when AToM is directly mapped to a traffic engineering (TE) tunnel.
- AToM is supported on the Cisco 7200 and 7500 series routers. For details on supported hardware, see the following documents:
  - [Cross-Platform Release Notes for Cisco IOS Release 12.0S](#)
  - [Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 2: Platform-Specific Information](#)
- AToM is supported on the Cisco 7600 routers. For details on supported shared port adapters and line cards, see the following documents:
  - [Guide to Supported Hardware for Cisco 7600 Series Routers with Release 12.2SR](#)
  - [Cross-Platform Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers](#)
- The Cisco 7600 router has platform-specific instructions for configuring some AToM features. Platform-specific configuration information is included in the following documents:
  - The “Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching” module of the [Cisco 7600 Series Cisco IOS Software Configuration Guide](#), Release 12.2SR
  - The “Configuring Multiprotocol Label Switching on the Optical Services Modules” module of the [OSM Configuration Note](#), Release 12.2SR
  - The “Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules” module of the [FlexWAN and Enhanced FlexWAN Modules Installation and Configuration Guides of Cisco 7600 Series Routers](#).
  - The “Configuring Any Transport over MPLS on a SIP” section of the [Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide](#)

- The “Configuring AToM VP Cell Mode Relay Support” section of the *Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide*
  - The *Cross-Platform Release Notes for Cisco IOS Release 12.2SR*
- AToM is supported on the Cisco 10000 series routers. For details on supported hardware, see the “Configuring Any Transport over MPLS” section of the *Cisco 10000 Series Router Software Configuration Guide*.
- The Cisco 10000 series router has platform-specific instructions for configuring some AToM features. Platform-specific configuration information is contained in the “Configuring Any Transport over MPLS” section of the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*.
- AToM is supported on the Cisco 12000 series routers. For information about hardware requirements, see the *Cross-Platform Release Notes for Cisco IOS Release 12.0S*.

## Restrictions for Any Transport over MPLS

The following general restrictions pertain to all transport types under AToM:

- Address format: Configure the Label Distribution Protocol (LDP) router ID on all PE routers to be a loopback address with a /32 mask. Otherwise, some configurations might not function properly.
- Layer 2 virtual private networks (L2VPN) features (AToM and Layer 2 Tunnel Protocol Version 3 (L2TPv3)) are not supported on an ATM interface.
- Distributed Cisco Express Forwarding is the only forwarding model supported on the Cisco 12000 series routers and is enabled by default. Disabling distributed Cisco Express Forwarding on the Cisco 12000 series routers disables forwarding.
- Distributed Cisco Express Forwarding mode is supported on the Cisco 7500 series routers for Frame Relay, HDLC, and PPP. In distributed Cisco Express Forwarding mode, the switching process occurs on the Versatile Interface Processors (VIPs) that support switching. When distributed Cisco Express Forwarding is enabled, VIP port adapters maintain identical copies of the Forwarding Information Base (FIB) and adjacency tables. The port adapters perform the express forwarding between port adapters, relieving the Route Switch Processor (RSP) from performing the switching. Distributed Cisco Express Forwarding uses an interprocess communications (IPC) mechanism to ensure synchronization of FIBs and adjacency tables between the RSP and port adapters.

The following restrictions pertain to ATM Cell Relay over MPLS:

- For ATM Cell Relay over MPLS, if you have TE tunnels running between the PE routers, you must enable LDP on the tunnel interfaces.
- Configuring ATM Relay over MPLS with the Cisco 12000 Series Router engine 2 8-port OC-3 STM-1 ATM line card: In Cisco IOS Release 12.0(25)S, there were special instructions for configuring ATM cell relay on the Cisco 12000 series router with an engine 2 8-port OC-3 STM-1 ATM line card. The special configuration instructions do not apply in releases later than Cisco IOS Release 12.0(25)S and you do not need to use the **atm mode cell-relay** command.

In Cisco IOS Release 12.0(25)S, when you configured the Cisco 12000 series 8-port OC-3 STM-1 ATM line card for ATM Cell Relay over MPLS, two ports were reserved. In releases later than Cisco IOS Release 12.0(25)S, only one port is reserved.

In addition, in Cisco IOS Release 12.0(25)S, if you configured an 8-port OC-3 STM-1 ATM port for ATM AAL5 over MPLS and then configured ATM single cell relay over MPLS on that port, the VCs and VPs for AAL5 on the port and its corresponding port were removed. Starting in Cisco IOS Release 12.0(26)S, this behavior no longer occurs. ATM AAL5 over MPLS and ATM single cell

relay over MPLS are supported on the same port. The Cisco 12000 series 8-port OC-3 STM-1 ATM line cards now support, by default, the ATM single cell relay over MPLS feature in both VP and VC modes and ATM AAL5 over MPLS on the same port.

- The F4 end-to-end OAM cells are transparently transported along with the ATM cells. When a permanent virtual path (PVP) or PVC is down on one PE router, the label associated with that PVP or PVC is withdrawn. Subsequently, the peer PE router detects the label withdrawal and sends an F4 AIS/RDI signal to its corresponding CE router. The PVP or PVC on the peer PE router remains in the up state.

The following restrictions pertain to the Ethernet over MPLS feature:

- Ethernet over MPLS supports VLAN packets that conform to the IEEE 802.1Q standard. The 802.1Q specification establishes a standard method for inserting VLAN membership information into Ethernet frames. The Inter-Switch Link (ISL) protocol is not supported between the PE and CE routers.
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.
- Ethernet packets with hardware-level cyclic redundancy check (CRC) errors, framing errors, and runt packets are discarded on input.
- In Cisco IOS Release 12.2(25)S, the behavior of the **mpls mtu** command changed. If the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).

**Caution**

Although you can set the MPLS MTU to a value greater than the interface MTU, set the MPLS MTU less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU rates.

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the command is rejected. See the [“Maximum Transmission Unit Guidelines for Estimating Packet Size” section on page 7](#) for more information.

The following restrictions pertain to the Frame Relay over MPLS feature:

- Frame Relay traffic shaping is not supported with AToM switched VCs.
- If you configure Frame Relay over MPLS on the Cisco 12000 series router and the core-facing interface is an engine 4 or 4+ line card and the edge-facing interface is an engine 0 or 2 line card, then the BECN, FECN, control word (CW), and DE bit information is stripped from the PVC.

# Information About Any Transport over MPLS

To configure AToM, you must understand the following concepts:

- [How AToM Transports Layer 2 Packets, page 5](#)
- [AToM Configuration Commands Prior to Cisco IOS Release 12.0\(25\)S, page 6](#)
- [Benefits of AToM, page 6](#)
- [MPLS Traffic Engineering Fast Reroute, page 6](#)
- [Maximum Transmission Unit Guidelines for Estimating Packet Size, page 7](#)
- [Frame Relay over MPLS and DTE, DCE, and NNI Connections, page 9](#)
- [QoS Features Supported with AToM, page 11](#)

## How AToM Transports Layer 2 Packets

AToM encapsulates Layer 2 frames at the ingress PE and sends them to a corresponding PE at the other end of a pseudowire, which is a connection between the two PE routers. The egress PE removes the encapsulation and sends out the Layer 2 frame.

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers. You specify the following information on each PE router:

- The type of Layer 2 data that will be transported across the pseudowire, such as Ethernet, Frame Relay, or ATM
- The IP address of the loopback interface of the peer PE router, which enables the PE routers to communicate
- A unique combination of peer PE IP address and VC ID that identifies the pseudowire

The following example shows the basic configuration steps on a PE router that enable the transport of Layer 2 packets. Each transport type has slightly different steps.

Step 1 defines the interface or subinterface on the PE router:

```
Router# interface interface-type interface-number
```

Step 2 specifies the encapsulation type for the interface, such as dot1q:

```
Router(config-if)# encapsulation encapsulation-type
```

Step 3 does the following:

- Makes a connection to the peer PE router by specifying the LDP router ID of the peer PE router.
- Specifies a 32-bit unique identifier, called the VC ID, which is shared between the two PE routers.  
The combination of the peer router ID and the VC ID must be unique on the router. Two circuits cannot use the same combination of peer router ID and VC ID.
- Specifies the tunneling method used to encapsulate data in the pseudowire. AToM uses MPLS as the tunneling method.

```
Router(config-if)# xconnect peer-router-id vcid encapsulation mpls
```

As an alternative, you can set up a pseudowire class to specify the tunneling method and other characteristics. See the [“Configuring the Pseudowire Class” section on page 15](#) for more information.

## AToM Configuration Commands Prior to Cisco IOS Release 12.0(25)S

In releases of AToM previous to Cisco IOS 12.0(25)S, the command used to configure AToM circuits was **mpls l2 transport route**. This command has been replaced with the **xconnect** command.

No enhancements will be made to the **mpls l2transport route** command. Enhancements will be made to either the **xconnect** command or **pseudowire-class** command. Therefore, Cisco recommends that you use the **xconnect** command to configure AToM circuits.

Configurations from releases previous to Cisco IOS 12.0(25)S that use the **mpls l2transport route** command are still supported.

## Benefits of AToM

The following list explains some of the benefits of enabling Layer 2 packets to be sent in the MPLS network:

- The AToM product set accommodates many types of Layer 2 packets, including Ethernet and Frame Relay, across multiple Cisco router platforms, such as the Cisco 7200 and 7500 series routers. This enables the service provider to transport all types of traffic over the backbone and accommodate all types of customers.
- AToM adheres to the standards developed for transporting Layer 2 packets over MPLS. (See the [“Standards” section on page 86](#) for the specific standards that AToM follows.) This benefits the service provider that wants to incorporate industry-standard methodologies in the network. Other Layer 2 solutions are proprietary, which can limit the service provider’s ability to expand the network and can force the service provider to use only one vendor’s equipment.
- Upgrading to AToM is transparent to the customer. Because the service provider network is separate from the customer network, the service provider can upgrade to AToM without disruption of service to the customer. The customers assume that they are using a traditional Layer 2 backbone.

## MPLS Traffic Engineering Fast Reroute

AToM can use MPLS traffic engineering (TE) tunnels with fast reroute (FRR) support. AToM VCs can be rerouted around a failed link or node at the same time as MPLS and IP prefixes.

Enabling fast reroute on AToM does not require any special commands; you can use standard fast reroute commands. At the ingress PE, an AToM tunnel is protected by fast reroute when it is routed to an FRR-protected TE tunnel. Both link and node protection are supported for AToM VCs at the ingress PE. For more information on configuring MPLS TE fast reroute, see the following document:

[\*MPLS Traffic Engineering \(TE\)—Link and Node Protection, with RSVP Hellos Support\*](#)



### Note

The AToM VC independence feature was introduced in Cisco IOS Release 12.0(31)S and enables the Cisco 12000 series router to perform fast reroute in fewer than 50 milliseconds, regardless of the number of VCs configured. In previous releases, the fast reroute time depended on the number of VCs inside the protected TE tunnel.

For the Cisco 12000 series routers, fast reroute uses three or more labels, depending on where the TE tunnel ends:

- If the TE tunnel is from a PE router to a PE router, three labels are used.



- If the TE tunnel is from a PE router to the core router, four labels are used.

Engine 0 ATM line cards support three or more labels, although performance degrades. Engine 2 Gigabit Ethernet line cards and engine 3 line cards support three or more labels and can work with the fast reroute feature.

You can issue the **debug mpls l2transport fast-reroute** command to debug fast reroute with AToM.



#### Note

This command does not display output on platforms where AToM fast reroute is implemented in the forwarding code. The command does display output on Cisco 10720 Internet router line cards and Cisco 12000 series line cards. This command does not display output for the Cisco 7500 (both Route Processor (RP) and VIP) series routers, Cisco 7200 series routers, and Cisco 12000 series RP.

In the following example, the primary link is disabled, which causes the backup tunnel (Tunnel 1) to become the primary path. In the following example, bolded output shows the status of the tunnel:

```
Router# execute-on slot 3 debug mpls l2transport fast-reroute
```

```
===== Line Card (Slot 3) =====
AToM fast reroute debugging is on
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Processing TFIB FRR event for 10.4.0.1
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Finished processing TFIB FRR event for 10.4.0.1
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Processing TFIB FRR event for Tunnel41
SLOT 3:Sep 16 17:58:56.346: AToM SMGR: Finished processing TFIB FRR event for Tunnel41
Sep 16 17:58:58.342: %LINK-3-UPDOWN: Interface POS0/0, changed state to down
Sep 16 17:58:58.342: %OSPF-5-ADJCHG: Process 1, Nbr 10.0.0.1 on POS0/0 from FULL to DOWN,
Neighbor Down: Interface down or detached
Sep 16 17:58:59.342: %LINEPROTO-5-UPDOWN: Line protocol on Interface POS0/0, changed state to down
```

## Maximum Transmission Unit Guidelines for Estimating Packet Size

The following calculation helps you determine the size of the packets traveling through the core network. You set the maximum transmission unit (MTU) on the core-facing interfaces of the P and PE routers to accommodate packets of this size. The MTU should be greater than or equal to the total bytes of the items in the following equation:

*Core MTU >= (Edge MTU + Transport header + AToM header + (MPLS label stack \* MPLS label size))*

The following sections describe the variables used in the equation:

### Edge MTU

The edge MTU is the MTU for the customer-facing interfaces.

### Transport Header

The Transport header depends on the transport type. [Table 1](#) lists the specific sizes of the headers.

**Table 1** Header Size of Packets

| Transport Type | Packet Size |
|----------------|-------------|
| AAL5           | 0–32 bytes  |
| Ethernet VLAN  | 18 bytes    |
| Ethernet Port  | 14 bytes    |

**Table 1**      **Header Size of Packets (continued)**

| Transport Type   | Packet Size                                                                                       |
|------------------|---------------------------------------------------------------------------------------------------|
| Frame Relay DLCI | 2 bytes for Cisco encapsulation, 8 bytes for Internet Engineering Task Force (IETF) encapsulation |
| HDLC             | 4 bytes                                                                                           |
| PPP              | 4 bytes                                                                                           |

**AToM Header**

The AToM header is 4 bytes (control word). The control word is optional for Ethernet, PPP, HDLC, and cell relay transport types. However, the control word is required for Frame Relay and ATM AAL5 transport types.

**MPLS Label Stack**

The MPLS label stack size depends on the configuration of the core MPLS network:

- AToM uses one MPLS label to identify the AToM VCs (VC label). Therefore, the minimum MPLS label stack is one for directly connected AToM PEs, which are PE routers that do not have a P router between them.
- If LDP is used in the MPLS network, the label stack size is two (the LDP label and the VC label).
- If a TE tunnel instead of LDP is used between PE routers in the MPLS network, the label stack size is two (the TE label and the VC label).
- If a TE tunnel and LDP are used in the MPLS network (for example, a TE tunnel between P routers or between P and PE routers, with LDP on the tunnel), the label stack is three (TE label, LDP label, VC label).
- If you use MPLS fast reroute in the MPLS network, you add a label to the stack. The maximum MPLS label stack in this case is four (FRR label, TE label, LDP label, VC label).
- If AToM is used by the customer carrier in an MPLS VPN Carrier Supporting Carrier environment, you add a label to the stack. The maximum MPLS label stack in the provider carrier network is five (FRR label, TE label, LDP label, VPN label, VC label).
- If an AToM tunnel spans different service providers that exchange MPLS labels using IPv4 Border Gateway Protocol (BGP) (RFC 3107), you add a label to the stack. The maximum MPLS label stack is five (FRR label, TE label, Border Gateway Protocol (BGP) label, LDP label, VC label).

Other circumstances can increase the MPLS label stack size. Therefore, analyze the complete data path between the AToM tunnel endpoints and determine the maximum MPLS label stack size for your network. Then multiply the label stack size by the size of the MPLS label.

**Estimating Packet Size: Example**

The size of packets is estimate in the following example, which uses the following assumptions:

- The edge MTU is 1500 bytes.
- The transport type is Ethernet VLAN, which designates 18 bytes for the transport header.
- The AToM header is 0, because the control word is not used.
- The MPLS label stack is 2, because LDP is used. The MPLS label is 4 bytes.

```
Edge MTU + Transport header + ATOM header + (MPLS label stack * MPLS label) = Core MTU
1500      + 18                + 0          + (2                * 4                ) = 1526
```

You must configure the P and PE routers in the core to accept packets of 1526 bytes.

Once you determine the MTU size to set on your P and PE routers, you can issue the **mtu** command on the routers to set the MTU size. The following example specifies an MTU of 1526 bytes:

```
Router(config-if)# mtu 1526
```

## mpls mtu Command Changes

Some interfaces (such as FastEthernet) require the **mpls mtu** command to change the MTU size. In Cisco IOS Release 12.2(25)S, the behavior of the **mpls mtu** command changed.

If the interface MTU is fewer than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).



### Caution

Although you can set the MPLS MTU to a value greater than the interface MTU, set the MPLS MTU less than or equal to the interface MTU to prevent data corruption, dropped packets, and high CPU rates.

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S and you have an MPLS MTU setting that does not conform to these guidelines, the command is rejected.

For Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases, you cannot set the MPLS MTU greater than the interface MTU. This eliminates problems, such as dropped packets, data corruption, and high CPU rates. See the [MPLS MTU Command Changes](#) document for more information.

## Frame Relay over MPLS and DTE, DCE, and NNI Connections

You can configure an interface as a DTE device or a DCE switch, or as a switch connected to a switch with network-to-network interface (NNI) connections. Use the following command in interface configuration mode:

```
frame-relay intf-type [dce | dte | nni]
```

The keywords are explained in [Table 2](#).

**Table 2** *frame-relay intf-type Command Keywords*

| Keyword    | Description                                                                          |
|------------|--------------------------------------------------------------------------------------|
| <b>dce</b> | Enables the router or access server to function as a switch connected to a router.   |
| <b>dte</b> | Enables the router or access server to function as a DTE device. DTE is the default. |
| <b>nni</b> | Enables the router or access server to function as a switch connected to a switch.   |

## Local Management Interface and Frame Relay over MPLS

Local Management Interface (LMI) is a protocol that communicates status information about PVCs. When a PVC is added, deleted, or changed, the LMI notifies the endpoint of the status change. LMI also provides a polling mechanism that verifies that a link is up.

### How LMI Works

To determine the PVC status, LMI checks that a PVC is available from the reporting device to the Frame Relay end-user device. If a PVC is available, LMI reports that the status is “Active,” which means that all interfaces, line protocols, and core segments are operational between the reporting device and the Frame Relay end-user device. If any of those components is not available, the LMI reports a status of “Inactive.”

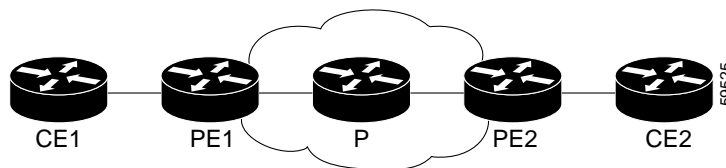


#### Note

Only the DCE and NNI interface types can report LMI status.

Figure 1 is a sample topology that helps illustrate how LMI works.

**Figure 1 Sample Topology**



In Figure 1, note the following:

- CE1 and PE1 and PE2 and CE2 are Frame Relay LMI peers.
- CE1 and CE2 can be Frame Relay switches or end-user devices.
- Each Frame Relay PVC comprises multiple segments.
- The DLCI value is local to each segment and is changed as traffic is switched from segment to segment. Two Frame Relay PVC segments exist in Figure 1; one is between PE1 and CE1 and the other is between PE2 and CE2.

The LMI protocol behavior depends on whether you have DLCI-to-DLCI or port-to-port connections.

#### DLCI-to-DLCI Connections

If you have DLCI-to-DLCI connections, LMI runs locally on the Frame Relay ports between the PE and CE devices:

- CE1 sends an active status to PE1 if the PVC for CE1 is available. If CE1 is a switch, LMI checks that the PVC is available from CE1 to the user device attached to CE1.
- PE1 sends an active status to CE1 if the following conditions are met:
  - A PVC for PE1 is available.
  - PE1 received an MPLS label from the remote PE router.
  - An MPLS tunnel label exists between PE1 and the remote PE.

For DTE or DCE configurations, the following LMI behavior exists: The Frame Relay device accessing the network (DTE) does not report PVC status. Only the network device (DCE) or NNI can report status. Therefore, if a problem exists on the DTE side, the DCE is not aware of the problem.

#### Port-to-Port Connections

If you have port-to-port connections, the PE routers do not participate in the LMI status-checking procedures. LMI operates between the CE routers only. The CE routers must be configured as DCE-DTE or NNI-NNI.

For information about LMI, including configuration instructions, see the “Configuring the LMI” section of the [Configuring Frame Relay](#) document.

## QoS Features Supported with AToM

For information about configuring QoS features on the Cisco 12000 series routers, see the following feature module:

*Any Transport over MPLS (AToM): Layer 2 QoS for the Cisco 12000 Series Router (Quality of Service)*

The following tables list the QoS features supported by AToM on the Cisco 7200 and 7500 series routers:

- [Table 3, QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers](#)
- [Table 4, QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers](#)
- [Table 5, QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers](#)

**Table 3** *QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | Ethernet over MPLS                                                                                                                                                                                                                                                                                             |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• Subinterface (input and output)</li> </ul>                                                                                                                                                                 |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match cos</b> (on interfaces and subinterfaces)</li> <li>• <b>match mpls experimental</b> (on interfaces and subinterfaces)</li> <li>• <b>match qos-group</b> (on interfaces) (output policy)</li> </ul>                          |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>set cos</b> (output policy)</li> <li>• <b>set discard-class</b> (input policy)</li> <li>• <b>set mpls experimental</b> (input policy) (on interfaces and subinterfaces)</li> <li>• <b>set qos-group</b> (input policy)</li> </ul> |

**Table 3** *QoS Features Supported with Ethernet over MPLS on the Cisco 7200 and 7500 Series Routers (continued)*

| QoS Feature          | Ethernet over MPLS                                                                                                                                                                                            |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>             |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• Distributed Low Latency Queueing (dLLQ)</li> <li>• Distributed Weighted Random Early Detection (dWRED)</li> <li>• Byte-based WRED</li> </ul> |

**Table 4** *QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | Frame Relay over MPLS                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• PVC (input and output)</li> </ul>                                                                                                                                                                                                                                               |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match fr-de</b> (on interfaces and VCs)</li> <li>• <b>match fr-dlci</b> (on interfaces)</li> <li>• <b>match qos-group</b></li> </ul>                                                                                                                                                                   |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>frame-relay congestion management</b> (output)</li> <li>• <b>set discard-class</b></li> <li>• <b>set fr-de</b> (output policy)</li> <li>• <b>set fr-fecn-becn</b> (output)</li> <li>• <b>set mpls experimental</b></li> <li>• <b>set qos-group</b></li> <li>• <b>threshold ecn</b> (output)</li> </ul> |

**Table 4** *QoS Features Supported with Frame Relay over MPLS on the Cisco 7200 and 7500 Series Routers (continued)*

| QoS Feature          | Frame Relay over MPLS                                                                                                                                                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>                                                                                                  |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• dLLQ</li> <li>• dWRED</li> <li>• Distributed traffic shaping</li> <li>• Distributed class-based weighted fair queueing (dCBWFQ)</li> <li>• Byte-based WRED</li> <li>• <b>random-detect discard-class-based</b> command</li> </ul> |

**Table 5** *QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature    | ATM Cell Relay and AAL5 over MPLS                                                                                                                                                                                                                                                                                                                                                            |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service policy | Can be applied to: <ul style="list-style-type: none"> <li>• Interface (input and output)</li> <li>• Subinterface (input and output)</li> <li>• PVC (input and output)</li> </ul>                                                                                                                                                                                                             |
| Classification | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>match mpls experimental</b> (on VCs)</li> <li>• <b>match qos-group</b> (output)</li> </ul>                                                                                                                                                                                                                      |
| Marking        | Supports the following commands: <ul style="list-style-type: none"> <li>• <b>random-detect discard-class-based</b> (input)</li> <li>• <b>set clp</b> (output) (on interfaces, subinterfaces, and VCs)</li> <li>• <b>set discard-class</b> (input)</li> <li>• <b>set mpls experimental</b> (input) (on interfaces, subinterfaces, and VCs)</li> <li>• <b>set qos-group</b> (input)</li> </ul> |

**Table 5** *QoS Features Supported with ATM Cell Relay and AAL5 over MPLS on the Cisco 7200 and 7500 Series Routers*

| QoS Feature          | ATM Cell Relay and AAL5 over MPLS                                                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Policing             | Supports the following: <ul style="list-style-type: none"> <li>• Single-rate policing</li> <li>• Two-rate policing</li> <li>• Color-aware policing</li> <li>• Multiple-action policing</li> </ul>                                                      |
| Queueing and shaping | Supports the following: <ul style="list-style-type: none"> <li>• dLLQ</li> <li>• dWRED</li> <li>• dCBWFQ</li> <li>• Byte-based WRED</li> <li>• random-detect discard-class-based command</li> <li>• Class-based shaping support on ATM PVCs</li> </ul> |

## How to Configure Any Transport over MPLS

This section explains how to perform a basic AToM configuration and includes the following procedures:

- [Configuring the Pseudowire Class, page 15](#) (required)
- [Changing the Encapsulation Type and Removing a Pseudowire, page 16](#) (optional)
- [Configuring ATM AAL5 over MPLS on PVCs, page 16](#) (optional)
- [Configuring ATM AAL5 over MPLS in VC Class Configuration Mode, page 18](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS, page 20](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs, page 21](#) (optional)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode, page 23](#) (optional)
- [Configuring ATM Cell Relay over MPLS in VC Mode, page 25](#) (optional)
- [Configuring ATM Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode, page 27](#) (optional)
- [Configuring ATM Cell Relay over MPLS in PVP Mode, page 28](#) (optional)
- [Configuring ATM Cell Relay over MPLS in Port Mode, page 30](#) (optional)
- [Configuring ATM Single Cell Relay over MPLS, page 33](#) (optional)
- [Configuring ATM Packed Cell Relay over MPLS, page 34](#) (optional)
- [Configuring Ethernet over MPLS in VLAN Mode, page 45](#) (optional)
- [Configuring Ethernet over MPLS in Port Mode, page 46](#) (optional)
- [Configuring Ethernet over MPLS with VLAN ID Rewrite, page 48](#) (optional)
- [Configuring per-Subinterface MTU for Ethernet over MPLS, page 52](#) (optional)



- [Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections, page 54](#) (optional)
- [Configuring Frame Relay over MPLS with Port-to-Port Connections, page 55](#) (optional)
- [Configuring HDLC and PPP over MPLS, page 56](#) (optional)
- [Configuring Tunnel Selection, page 58](#) (optional)
- [Setting Experimental Bits with AToM, page 61](#) (optional)
- [Setting the Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers, page 65](#) (optional)
- [Matching the Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers, page 66](#) (optional)
- [Enabling the Control Word, page 66](#)

## Configuring the Pseudowire Class

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers.



### Note

In simple configurations, this task is optional. You do not need to specify a pseudowire class if you specify the tunneling method as part of the **xconnect** command.

The pseudowire-class configuration group specifies the following characteristics of the tunneling mechanism:

- Encapsulation type
- Control protocol
- Payload-specific options

For more information about the **pseudowire-class** command, see the following feature module: [Layer 2 Tunnel Protocol Version 3](#).

You must specify the **encapsulation mpls** command as part of the pseudowire class or as part of the **xconnect** command for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **xconnect** command, you receive the following error:

```
% Incomplete command.
```

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                |
| Step 3 | <b>pseudowire-class</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.      |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw-class)#<br>encapsulation mpls  | Specifies the tunneling encapsulation.                                                                           |

## Changing the Encapsulation Type and Removing a Pseudowire

To change the type of encapsulation, remove the pseudowire with the **no pseudowire-class** command and reestablish the pseudowire and specify the new encapsulation type.

Once you specify the **encapsulation mpls** command, you cannot remove it using the **no encapsulation mpls** command. Nor can you change the command's setting using the **encapsulation l2tpv3** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove a pseudowire, use the **clear xconnect** command in privileged EXEC command. You can remove all pseudowires or specific pseudowires on an interface or peer router.

## Configuring ATM AAL5 over MPLS on PVCs

ATM AAL5 over MPLS for permanent virtual circuits encapsulates ATM AAL5 service data unit (SDUs) in MPLS packets and forwards them across the MPLS network. Each ATM AAL5 SDU is transported as a single packet.

### Restrictions

AAL5 over MPLS is supported only in SDU mode.

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
  - a. **interface** *typeslot/port*
3. **pvc** [*name*] *vpi/vci* **l2transport**
4. **encapsulation aal5**
5. **xconnect** *peer-router-id vcid* **encapsulation mpls**
6. **exit**
7. **exit**
8. **exit**
9. **show mpls l2transport vc**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                             | Purpose                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                | Enters global configuration mode.                                                                                                                                                                                                         |
| Step 3 | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atml/0                                                                              | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                          |
| Step 4 | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                               | Creates or assigns a name to an ATM PVC and enters L2transport configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| Step 5 | <b>encapsulation aal5</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal5                                                                     | Specifies ATM AAL5 encapsulation for the PVC. <ul style="list-style-type: none"> <li>Make sure that you specify the same encapsulation type on the PE and customer edge (CE) routers.</li> </ul>                                          |
| Step 6 | <b>xconnect</b> <i>peer-router-id vcid</i> <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                          |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                                 | Exits L2transport configuration mode.                                                                                                                                                                                                     |

|         |                                                                                                 |                                                                       |
|---------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| Step 8  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                              | Exits interface configuration mode.                                   |
| Step 9  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config)# exit</p>                                 | Exits global configuration mode.                                      |
| Step 10 | <pre>show mpls l2transport vc</pre> <p><b>Example:</b><br/>Router# show mpls l2transport vc</p> | Displays output that shows ATM AAL5 over MPLS is configured on a PVC. |

## Examples

The following is sample output from the **show mpls l2transport vc** command, which shows that ATM AAL5 over MPLS is configured on a PVC:

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit  | Dest address | VC ID | Status |
|------------|----------------|--------------|-------|--------|
| -----      | -----          | -----        | ----- | -----  |
| ATM1/0     | ATM AAL5 1/100 | 10.4.4.4     | 100   | UP     |

## Configuring ATM AAL5 over MPLS in VC Class Configuration Mode

You can create a VC class that specifies the AAL5 encapsulation and then attach the encapsulation type to an interface, subinterface, or PVC. The following task creates a VC class and attaches it to a main interface.

## Restrictions

AAL5 over MPLS is supported only in SDU mode.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *vc-class-name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *typeslot/port*
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi/vci* **l2transport**
9. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
10. **exit**

11. **exit**
12. **exit**
13. **show atm class-links**

## DETAILED STEPS

|        | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                            |
| Step 3 | <b>vc-class atm vc-class-name</b><br><br><b>Example:</b><br>Router(config)# vc-class atm aal5class                                                              | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                   |
| Step 4 | <b>encapsulation layer-type</b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal5                                                           | Configures the AAL and encapsulation type.                                                                                                                                                                                                   |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                                                             | Exits VC class configuration mode.                                                                                                                                                                                                           |
| Step 6 | <b>interface typeslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                       | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                             |
| Step 7 | <b>class-int vc-class-name</b><br><br><b>Example:</b><br>Router(config-if)# class-int aal5class                                                                 | Applies a VC class to the ATM main interface or subinterface.<br><br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                     |
| Step 8 | <b>pvc [name] vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                        | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| Step 9 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                             |

|                |                                                                         |                                                                                       |
|----------------|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>Step 10</b> | <code>exit</code>                                                       | Exits L2transport configuration mode.                                                 |
|                | <b>Example:</b><br><code>Router(config-if-atm-l2trans-pvc)# exit</code> |                                                                                       |
| <b>Step 11</b> | <code>exit</code>                                                       | Exits interface configuration mode.                                                   |
|                | <b>Example:</b><br><code>Router(config-if)# exit</code>                 |                                                                                       |
| <b>Step 12</b> | <code>exit</code>                                                       | Exits global configuration mode.                                                      |
|                | <b>Example:</b><br><code>Router(config)# exit</code>                    |                                                                                       |
| <b>Step 13</b> | <code>show atm class-links</code>                                       | Displays the type of encapsulation and that the VC class was applied to an interface. |
|                | <b>Example:</b><br><code>Router# show atm class-links</code>            |                                                                                       |

## Examples

In the following example, the command output of the **show atm class-links** command verifies that ATM AAL5 over MPLS is configured as part of a VC class. The command output shows the type of encapsulation and that the VC class was applied to an interface.

```
Router# show atm class-links 1/100
```

```
Displaying vc-class inheritance for ATM1/0.0, vc 1/100:
no broadcast - Not configured - using default
encapsulation aal5 - VC-class configured on main interface
```

## Configuring OAM Cell Emulation for ATM AAL5 over MPLS

If a PE router does not support the transport of Operation, Administration, and Maintenance (OAM) cells across a label switched path (LSP), you can use OAM cell emulation to locally terminate or loop back the OAM cells. You configure OAM cell emulation on both PE routers, which emulates a VC by forming two unidirectional LSPs. You use the **oam-ac emulation-enable** and **oam-pvc manage** commands on both PE routers to enable OAM cell emulation.

After you enable OAM cell emulation on a router, you can configure and manage the ATM VC in the same manner as you would a terminated VC. A VC that has been configured with OAM cell emulation can send loopback cells at configured intervals toward the local CE router. The endpoint can be either of the following:

- End-to-end loopback, which sends OAM cells to the local CE router.
- Segment loopback, which responds to OAM cells to a device along the path between the PE and CE routers.

The OAM cells include the following cells:

- Alarm indication signal (AIS)
- Remote defect indication (RDI)

These cells identify and report defects along a VC. When a physical link or interface failure occurs, intermediate nodes insert OAM AIS cells into all the downstream devices affected by the failure. When a router receives an AIS cell, it marks the ATM VC down and sends an RDI cell to let the remote end know about the failure.

This section contains two tasks:

- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs, page 21](#)
- [Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode, page 23](#)

## Configuring OAM Cell Emulation for ATM AAL5 over MPLS on PVCs

Perform this task to configure OAM cell emulation for ATM AAL5 over MPLS on a PVC.



### Note

For AAL5 over MPLS, you can configure the **oam-pvc manage** command only after you issue the **oam-ac emulation-enable** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *typeslot/port*
4. **pvc** [*name*] *vpi/vci* **l2transport**
5. **encapsulation aal5**
6. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**
7. **oam-ac emulation-enable** [*ais-rate*]
8. **oam-pvc manage** [*frequency*]
9. **exit**
10. **exit**
11. **exit**
12. **show atm pvc**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                       |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                                     | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                                                              |
| Step 4 | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                      | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                  |
| Step 5 | <b>encapsulation aal5</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal5                                                                            | Specifies ATM AAL5 encapsulation for the PVC. <ul style="list-style-type: none"> <li>Make sure you specify the same encapsulation type on the PE and CE routers.</li> </ul>                                                                                                                                                   |
| Step 6 | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                                                              |
| Step 7 | <b>oam-ac emulation-enable</b> [ <i>ais-rate</i> ]<br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# oam-ac emulation-enable 30                                           | Enables OAM cell emulation for AAL5 over MPLS. <ul style="list-style-type: none"> <li>The <i>ais-rate</i> argument lets you specify the rate at which AIS cells are sent. The default is one cell every second. The range is 0 to 60 seconds.</li> </ul>                                                                      |
| Step 8 | <b>oam-pvc manage</b> [ <i>frequency</i> ]<br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# oam-pvc manage                                                               | Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit. <ul style="list-style-type: none"> <li>The optional <i>frequency</i> argument is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds.</li> </ul> |
| Step 9 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                                        | Exits L2transport configuration mode.                                                                                                                                                                                                                                                                                         |



|                |                                                                    |                                                                          |
|----------------|--------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 10</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit      | Exits interface configuration mode.                                      |
| <b>Step 11</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit         | Exits global configuration mode.                                         |
| <b>Step 12</b> | <b>show atm pvc</b><br><br><b>Example:</b><br>Router# show atm pvc | Displays output that shows OAM cell emulation is enabled on the ATM PVC. |

## Examples

The output of the **show atm pvc** command in the following example shows that OAM cell emulation is enabled on the ATM PVC:

```
Router# show atm pvc 5/500
```

```
ATM4/1/0.200: VCD: 6, VPI: 5, VCI: 500
UBR, PeakRate: 1
AAL5-LLC/SNAP, etype:0x0, Flags: 0x34000C20, VCmode: 0x0
OAM Cell Emulation: enabled, F5 End2end AIS Xmit frequency: 1 second(s)
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state: Not ManagedVerified
ILMI VC state: Not Managed
InPkts: 564, OutPkts: 560, InBytes: 19792, OutBytes: 19680
InPRoc: 0, OutPRoc: 0
InFast: 4, OutFast: 0, InAS: 560, OutAS: 560
InPktDrops: 0, OutPktDrops: 0
CrcErrors: 0, SarTimeOuts: 0, OverSizedSDUs: 0
Out CLP=1 Pkts: 0
OAM cells received: 26
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 26
OAM cells sent: 77
F5 OutEndloop: 0, F5 OutSegloop: 0, F5 OutAIS: 77, F5 OutRDI: 0
OAM cell drops: 0
Status: UP
```

## Configuring OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode

The following steps explain how to configure OAM cell emulation as part of a VC class. You can then apply the VC class to an interface, a subinterface, or a VC. When you configure OAM cell emulation in VC class configuration mode and then apply the VC class to an interface, the settings in the VC class apply to all the VCs on the interface, unless you specify a different OAM cell emulation value at a lower level, such as the subinterface or VC level. For example, you can create a VC class that specifies OAM cell emulation and sets the rate of AIS cells to every 30 seconds. You can apply the VC class to an interface. Then, for one PVC, you can enable OAM cell emulation and set the rate of AIS cells to every 15 seconds. All the PVCs on the interface use the cell rate of 30 seconds, except for the one PVC that was set to 15 seconds.

Perform this task to enable OAM cell emulation as part of a VC class and apply it to an interface.

**Note**

For AAL5 over MPLS, you can configure the **oam-pvc manage** command only after you issue the **oam-ac emulation-enable** command.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **vc-class atm *name***
4. **encapsulation *layer-type***
5. **oam-ac emulation-enable [*ais-rate*]**
6. **oam-pvc manage [*frequency*]**
7. **exit**
8. **interface *typeslot/port***
9. **class-int *vc-class-name***
10. **pvc [*name*] vpi/vci l2transport**
11. **xconnect *peer-router-id vcid encapsulation mpls***

**DETAILED STEPS**

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                 | Enters global configuration mode.                                                                                                                                                                                                                         |
| Step 3 | <b>vc-class atm <i>name</i></b><br><br><b>Example:</b><br>Router(config)# vc-class atm oamclass                                | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                                |
| Step 4 | <b>encapsulation <i>layer-type</i></b><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal5                   | Configures the AAL and encapsulation type.                                                                                                                                                                                                                |
| Step 5 | <b>oam-ac emulation-enable [<i>ais-rate</i>]</b><br><br><b>Example:</b><br>Router(config-vc-class)# oam-ac emulation-enable 30 | Enables OAM cell emulation for AAL5 over MPLS.<br><ul style="list-style-type: none"><li>The <i>ais-rate</i> argument lets you specify the rate at which AIS cells are sent. The default is one cell every second. The range is 0 to 60 seconds.</li></ul> |

|                |                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b>  | <code>oam-pvc manage [frequency]</code><br><br><b>Example:</b><br>Router(config-vc-class)# oam-pvc manage                                                             | Enables the PVC to generate end-to-end OAM loopback cells that verify connectivity on the virtual circuit. <ul style="list-style-type: none"> <li>The optional <i>frequency</i> argument is the interval between transmission of loopback cells and ranges from 0 to 600 seconds. The default value is 10 seconds.</li> </ul> |
| <b>Step 7</b>  | <code>exit</code><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                                                             | Exits VC class configuration mode.                                                                                                                                                                                                                                                                                            |
| <b>Step 8</b>  | <code>interface typeslot/port</code><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                       | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                                                              |
| <b>Step 9</b>  | <code>class-int vc-class-name</code><br><br><b>Example:</b><br>Router(config-if)# class-int oamclass                                                                  | Applies a VC class to the ATM main interface or subinterface.<br><br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                                                                                                      |
| <b>Step 10</b> | <code>pvc [name] vpi/vci l2transport</code><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                        | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                  |
| <b>Step 11</b> | <code>xconnect peer-router-id vcid encapsulation mpls</code><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                                                              |

## Configuring ATM Cell Relay over MPLS in VC Mode

Perform this task to configure ATM cell relay on the permanent virtual circuits.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm***slot/port*
4. **pvc** *vpi/vci* **l2transport**
5. **encapsulation aal0**
6. **xconnect** *peer-router-id vcid* **encapsulation mpls**
7. **exit**
8. **exit**
9. **exit**
10. **show atm vc**

## DETAILED STEPS

|         | Command or Action                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                  |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                  | Enters global configuration mode.                                                                                                                                                                                                                                               |
| Step 3  | <b>interface atmslot/port</b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                                        | Specifies an ATM interface and enters interface configuration mode.                                                                                                                                                                                                             |
| Step 4  | <b>pvc vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 0/100 l2transport                                                               | Assigns a virtual path identifier (VPI) and virtual circuit identifier (VCI) and enters L2transport VC configuration mode. <ul style="list-style-type: none"><li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li></ul> |
| Step 5  | <b>encapsulation aal0</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal0                                                       | For ATM cell relay, specifies raw cell encapsulation for the interface. <ul style="list-style-type: none"><li>Make sure you specify the same encapsulation type on the PE and CE routers.</li></ul>                                                                             |
| Step 6  | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                |
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                   | Exits L2transport configuration mode.                                                                                                                                                                                                                                           |
| Step 8  | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                   | Exits interface configuration mode.                                                                                                                                                                                                                                             |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                      | Exits global configuration mode.                                                                                                                                                                                                                                                |
| Step 10 | <b>show atm vc</b><br><br><b>Example:</b><br>Router# show atm vc                                                                                                | Verifies that OAM cell emulation is enabled on the ATM VC.                                                                                                                                                                                                                      |

## Examples

The output of the **show atm vc** command shows that the interface is configured for VC mode cell relay:

```
Router# show atm vc 7

ATM3/0: VCD: 7, VPI: 23, VCI: 100
UBR, PeakRate: 149760
AAL0-Cell Relay, etype:0x10, Flags: 0x10000C2D, VCmode: 0x0
OAM Cell Emulation: not configured
InBytes: 0, OutBytes: 0
Status: UP
```

## Configuring ATM Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

You can create a VC class that specifies the ATM cell relay encapsulation and then attach the VC class to an interface, subinterface, or VC. The following task creates a VC class that specifies the ATM cell relay encapsulation and attaches it to a main interface.



### Note

You can configure VC class configuration mode only in VC mode. VC class configuration mode is not supported on VP or port mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **encapsulation** *layer-type*
5. **exit**
6. **interface** *typeslot/port*
7. **class-int** *vc-class-name*
8. **pvc** [*name*] *vpi/vci* **l2transport**
9. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |

|               |                                                                                                   |                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>vc-class</b> <i>atm name</i>                                                                   | Creates a VC class and enters VC class configuration mode.                                                                                             |
|               | <b>Example:</b><br>Router(config)# vc-class atm cellrelay                                         |                                                                                                                                                        |
| <b>Step 4</b> | <b>encapsulation</b> <i>layer-type</i>                                                            | Configures the AAL and encapsulation type.                                                                                                             |
|               | <b>Example:</b><br>Router(config-vc-class)# encapsulation aal0                                    |                                                                                                                                                        |
| <b>Step 5</b> | <b>exit</b>                                                                                       | Exits VC class configuration mode.                                                                                                                     |
|               | <b>Example:</b><br>Router(config-vc-class)# exit                                                  |                                                                                                                                                        |
| <b>Step 6</b> | <b>interface</b> <i>typeslot/port</i>                                                             | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                       |
|               | <b>Example:</b><br>Router(config)# interface atm1/0                                               |                                                                                                                                                        |
| <b>Step 7</b> | <b>class-int</b> <i>vc-class-name</i>                                                             | Applies a VC class to the ATM main interface or subinterface.                                                                                          |
|               | <b>Example:</b><br>Router(config-if)# class-int cellrelay                                         | <b>Note</b> You can also apply a VC class to a PVC.                                                                                                    |
| <b>Step 8</b> | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b>                                      | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode.                                                                  |
|               | <b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                       | <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| <b>Step 9</b> | <b>xconnect</b> <i>peer-router-id vcid</i> <b>encapsulation mpls</b>                              | Binds the attachment circuit to a pseudowire VC.                                                                                                       |
|               | <b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls |                                                                                                                                                        |

## Configuring ATM Cell Relay over MPLS in PVP Mode

VP mode allows cells coming into a predefined PVP on the ATM interface to be transported over the MPLS backbone to a predefined PVP on the egress ATM interface. You can use VP mode to send single cells or packed cells over the MPLS backbone.

To configure VP mode, you must specify the following:

- The VP for transporting cell relay cells.
- The IP address of the peer PE router and the VC ID.

When configuring ATM cell relay over MPLS in VP mode, use the following guidelines:

- You do not need to enter the **encapsulation aal0** command in VP mode.
- One ATM interface can accommodate multiple types of ATM connections. VP cell relay, VC cell relay, and ATM AAL5 over MPLS can coexist on one ATM interface. On the Cisco 12000 series router, this is true only on the engine 0 ATM line cards.
- If a VPI is configured for VP cell relay, you cannot configure a PVC using the same VPI.

- VP trunking (mapping multiple VPs to one emulated VC label) is not supported. Each VP is mapped to one emulated VC.
- Each VP is associated with one unique emulated VC ID. The AToM emulated VC type is ATM VP cell transport.
- The AToM control word is supported. However, if a peer PE does not support the control word, it is disabled. This negotiation is done by LDP label binding.
- VP mode (and VC mode) drop idle cells.

Perform this task to configure ATM cell relay in PVP mode.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm***slot/port*
4. **atm pvp** *vpi* **l2transport**
5. **xconnect** *peer-router-id* **vcid** **encapsulation mpls**
6. **exit**
7. **exit**
8. **exit**
9. **show atm vp**

## DETAILED STEPS

|        | Command or Action                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>interface atm</b> <i>slot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0                              | Defines the interface and enters interface configuration mode.                                                                                                                                                                                                                                                        |
| Step 4 | <b>atm pvp</b> <i>vpi</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# <b>atm pvp</b> 1 <b>l2transport</b> | Specifies that the PVP is dedicated to transporting ATM cells and enters l2transport PVP configuration submode.<br><ul style="list-style-type: none"><li>• The <b>l2transport</b> keyword indicates that the PVP is for cell relay. This submode is for Layer 2 transport only; it is not for regular PVPs.</li></ul> |

|        | Command or Action                                                                                                                                                                              | Purpose                                                                                                                                                                         |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i><br><b>encapsulation</b> <b>mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvp)#<br>xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# exit                                                                                                                  | Exits L2 transport configuration mode.                                                                                                                                          |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                                                  | Exits interface configuration mode.                                                                                                                                             |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                     | Exits global configuration mode.                                                                                                                                                |
| Step 9 | <b>show atm vp</b><br><br><b>Example:</b><br>Router# show atm vp                                                                                                                               | Displays output that shows OAM cell emulation is enabled on the ATM VP.                                                                                                         |

## Examples

The following **show atm vp** command in the following example shows that the interface is configured for VP mode cell relay:

```
Router# show atm vp 1
```

```
ATM5/0 VPI: 1, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status:
ACTIVE
```

| VCD | VCI | Type | InPkts | OutPkts | AAL/Encap | Status |
|-----|-----|------|--------|---------|-----------|--------|
| 6   | 3   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |
| 7   | 4   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |

```
TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,
TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0
```

## Configuring ATM Cell Relay over MPLS in Port Mode

Port mode cell relay allows cells coming into an ATM interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress ATM interface.

To configure port mode, issue the **xconnect** command from an ATM main interface and specify the destination address and the VC ID. The syntax of the **xconnect** command is the same as for all other transport types. Each ATM port is associated with one unique pseudowire VC label.

When configuring ATM cell relay over MPLS in port mode, use the following guidelines:



- The pseudowire VC type is set to ATM transparent cell transport (AAL0).
- The AToM control word is supported. However, if the peer PE does not support a control word, the control word is disabled. This negotiation is done by LDP label binding.



**Note** The AToM control word is not supported for port mode cell relay on Cisco 7600 series routers.

- Port mode and VP and VC mode are mutually exclusive. If you enable an ATM main interface for cell relay, you cannot enter any PVP or PVC commands.
- If the pseudowire VC label is withdrawn due to an MPLS core network failure, the PE router sends a line AIS to the CE router.
- For the Cisco 7600 series routers, you must specify the interface ATM slot, bay, and port for the SIP400 or SIP200.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *atmslot/port*  
or  
**interface** *atmslot/bay/port*
4. **xconnect** *peer-router-id vcid encapsulation mpls*
5. **exit**
6. **exit**
7. **show atm route**
8. **show mpls l2transport vc**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                          |
| Step 3 | <b>interface</b> <i>atmslot/port</i><br>or<br><b>interface</b> <i>atmslot/bay/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0<br>or<br>Router(config)# interface atm4/3/0 | Specifies an ATM interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>• For the Cisco 7600 series routers, you must specify the interface ATM slot, bay, and port for the SIP400 or SIP200. In the example the slot is 4, the bay is 3, and the port is 0.</li> </ul> |

|               |                                                                                                                                                       |                                                                          |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| <b>Step 4</b> | <code>xconnect peer-router-id vcid encapsulation mpls</code><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123<br>encapsulation mpls | Binds the attachment circuit to the interface.                           |
| <b>Step 5</b> | <code>exit</code><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                   | Exits interface configuration mode.                                      |
| <b>Step 6</b> | <code>exit</code><br><br><b>Example:</b><br>Router(config)# exit                                                                                      | Exits global configuration mode.                                         |
| <b>Step 7</b> | <code>show atm route</code><br><br><b>Example:</b><br>Router# show atm route                                                                          | Displays output that shows ATM cell relay in port mode has been enabled. |
| <b>Step 8</b> | <code>show mpls l2transport vc</code><br><br><b>Example:</b><br>Router# show mpls l2transport vc                                                      | Displays the attachment circuit and the interface.                       |

## Examples

The **show atm route** command in the following example displays port mode cell relay state. The following example shows that atm interface 1/0 is for cell relay, the VC ID is 123 and the tunnel is down.

Router# **show atm route**

| Input Intf | Output Intf | Output VC | Status |
|------------|-------------|-----------|--------|
| ATM1/0     | ATOM Tunnel | 123       | DOWN   |

The **show mpls l2transport vc** command in the following example also shows configuration information:

Router# **show mpls l2transport vc**

| Local intf | Local circuit   | Dest address | VC ID | Status |
|------------|-----------------|--------------|-------|--------|
| AT1/0      | ATM CELL ATM1/0 | 10.1.1.121   | 1121  | UP     |

## Troubleshooting Tips

The **debug atm l2transport** and **debug mpls l2transport vc** display troubleshooting information.

## Configuring ATM Single Cell Relay over MPLS

The single cell relay feature allows you to insert one ATM cell in each MPLS packet. You can use single cell relay in both VP and VC mode. The configuration steps show how to configure single cell relay in VC mode. For VP mode, see the [“Configuring ATM Cell Relay over MPLS in PVP Mode”](#) section on page 28.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm<sup>slot/port</sup>**
4. **pvc vpi/vci l2transport**
5. **encapsulation aal0**
6. **xconnect peer-router-id vcid encapsulation mpls**

### DETAILED STEPS

|        | Command or Action                                                                                                                                            | Purpose                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                       | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                               | Enters global configuration mode.                                                                                                                                                                                               |
| Step 3 | <b>interface atm<sup>slot/port</sup></b><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                          | Specifies an ATM interface and enters interface configuration mode.                                                                                                                                                             |
| Step 4 | <b>pvc vpi/vci l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/100 l2transport                                                            | Assigns a VPI and VCI and enters L2transport VC configuration mode.<br><ul style="list-style-type: none"> <li>• The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul> |
| Step 5 | <b>encapsulation aal0</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# encapsulation aal0                                                    | Specifies raw cell encapsulation for the interface.<br><ul style="list-style-type: none"> <li>• Make sure you specify the same encapsulation type on the PE and CE routers.</li> </ul>                                          |
| Step 6 | <b>xconnect peer-router-id vcid encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                |

## Configuring ATM Packed Cell Relay over MPLS

The packed cell relay feature allows you to insert multiple concatenated ATM cells in an MPLS packet. The packed cell relay feature is more efficient than single cell relay, because each ATM cell is 52 bytes, and each AToM packet is at least 64 bytes.

At a high level, packed cell relay configuration consists of the following steps:

1. You specify the amount of time a PE router can wait for cells to be packed into an MPLS packet. You can set up three timers by default with different amounts of time attributed to each timer.
2. You enable packed cell relay, specify how many cells should be packed into each MPLS packet, and choose which timer to use during the cell packing process.

### Restrictions

- The **cell-packing** command is available only if you use AAL0 encapsulation in VC mode. If the command is configured with ATM AAL5 encapsulation, the command is not valid.
- Only cells from the same VC, VP, or port can be packed into one MPLS packet. Cells from different connections cannot be concatenated into the same MPLS packet.
- When you change, enable, or disable the cell-packing attributes, the ATM VC, VP, or port and the MPLS emulated VC are reestablished.
- If a PE router does not support packed cell relay, the PE router sends only one cell per MPLS packet.
- The number of packed cells does not need to match between the PE routers. The two PE routers agree on the lower of the two values. For example, if PE1 is allowed to pack 10 cells per MPLS packet and PE2 is allowed to pack 20 cells per MPLS packet, the two PE routers would agree to send no more than 10 cells per packet.
- If the number of cells packed by the peer PE router exceeds the limit, the packet is dropped.
- Issue the **atm mcpt-timers** command on an ATM interface before issuing the **cell-packing** command.

See the following sections for configuration information:

- [Configuring ATM Packed Cell Relay over MPLS in VC Mode, page 34](#)
- [Configuring ATM Packed Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode, page 37](#)
- [Configuring ATM Packed Cell Relay over MPLS in VP Mode, page 40](#)
- [Configuring ATM Packed Cell Relay over MPLS in Port Mode, page 42](#)

### Configuring ATM Packed Cell Relay over MPLS in VC Mode

Perform this task to configure the ATM packed cell relay over MPLS feature in VC mode.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm***slot/port*
4. **shutdown**

5. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
6. **no shutdown**
7. **pvc vpi/vci l2transport**
8. **encapsulation aal0**
9. **xconnect peer-router-id vcid encapsulation mpls**
10. **cell-packing** [*cells*] [**mcpt-timer** *timer*]

## DETAILED STEPS

|        | Command or Action                                   | Purpose                                                                            |
|--------|-----------------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                       | Enables privileged EXEC mode.                                                      |
|        | <b>Example:</b><br>Router> enable                   | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                           | Enters global configuration mode.                                                  |
|        | <b>Example:</b><br>Router# configure terminal       |                                                                                    |
| Step 3 | <b>interface atm slot/port</b>                      | Defines the interface and enters interface configuration mode.                     |
|        | <b>Example:</b><br>Router(config)# interface atm1/0 |                                                                                    |
| Step 4 | <b>shutdown</b>                                     | Shuts down the interface.                                                          |
|        | <b>Example:</b><br>Router(config-if)# shutdown      |                                                                                    |

|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>atm mcpt-timers</b> [<i>timer1-timeout timer2-timeout timer3-timeout</i>]</p> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p> | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <ul style="list-style-type: none"> <li>You can set up to three timers. For each timer, you specify the maximum cell-packing timeout (MCPT). This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</li> <li>The respective default values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> </li> <li>You can specify either the number of microseconds or use the default.</li> <li>The respective range of values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> </li> </ul> |
| Step 6 | <p><b>no shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                           | Enables the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 7 | <p><b>pvc vpi/vci l2transport</b></p> <p><b>Example:</b><br/>Router(config-if)# pvc 1/100 l2transport</p>                                                     | <p>Assigns a VPI and VCI and enters L2transport VC configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 8 | <p><b>encapsulation aa10</b></p> <p><b>Example:</b><br/>Router(config-if-atm-l2trans-pvc)# encapsulation aa10</p>                                             | <p>Specifies raw cell encapsulation for the interface.</p> <ul style="list-style-type: none"> <li>Make sure you specify the same encapsulation type on the PE routers.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|         | Command or Action                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> <b>encapsulation mpls</b>                       | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                                                                                                                                                        |
|         | <b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect<br>10.0.0.1 123 encapsulation mpls |                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 10 | <b>cell-packing</b> [ <i>cells</i> ] [ <b>mcpt-timer</b> <i>timer</i> ]                           | Enables cell packing and specifies the cell-packing parameters.                                                                                                                                                                                                                                                                                                                                                         |
|         | <b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# cell-packing<br>10 mcpt-timer 1             | <ul style="list-style-type: none"> <li>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.</li> <li>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.</li> <li>See the <b>cell-packing</b> command page for more information.</li> </ul> |

## Configuring ATM Packed Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

You can create a VC class that specifies the ATM cell relay encapsulation and the cell packing parameters and then attach the VC class to an interface, subinterface, or VC. The following task creates a VC class that specifies the ATM cell relay encapsulation and cell packing and attaches it to a main interface.



### Note

You can configure VC class configuration mode only in VC mode. VC class configuration mode is not supported on VP or port mode.

When you configure cell packing in VC class configuration mode and then apply the VC class to an interface, the settings in the VC class apply to all the VCs on the interface, unless you specify a different cell packing value at a lower level, such as the subinterface or VC level. For example, you can create a VC class that specifies three cells to be packed. You can apply the VC class to an interface. Then, for one PVC, you can specify two cells to be packed. All the PVCs on the interface pack three cells, except for the one PVC that was set to set two cells.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vc-class atm** *name*
4. **encapsulation** *layer-type*
5. **cell-packing** [*cells*] [**mcpt-timer** *timer*]
6. **exit**
7. **interface** *typeslot/port*
8. **shutdown**
9. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]

10. **no shutdown**
11. **class-int** *vc-class-name*
12. **pvc** [*name*] *vpi/vci* **l2transport**
13. **xconnect** *peer-router-id* *vcid* **encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 3 | <b>vc-class</b> <i>atm name</i><br><br><b>Example:</b><br>Router(config)# vc-class atm cellpacking                                                         | Creates a VC class and enters VC class configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <b>encapsulation</b> <i>layer-type</i><br><br><b>Example:</b><br>Router(config-vc-class)# encapsulation aal0                                               | Configures the AAL and encapsulation type.                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 5 | <b>cell-packing</b> [ <i>cells</i> ] [ <b>mcpt-timer</b> <i>timer</i> ]<br><br><b>Example:</b><br>Router(config-vc-class)# cell-packing 10<br>mcpt-timer 1 | Enables cell packing and specifies the cell-packing parameters. <ul style="list-style-type: none"><li>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.</li><li>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.</li><li>See the <b>cell-packing</b> command page for more information.</li></ul> |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vc-class)# exit                                                                                        | Exits VC class configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 7 | <b>interface</b> <i>typeslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0                                                           | Specifies the interface by type, slot, and port number, and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                    |



|                |                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 8</b>  | <b>shutdown</b><br><br><b>Example:</b><br>Router(config-if)# shutdown                                                                                                                       | Shuts down the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 9</b>  | <b>atm mcpt-timers</b> [timer1-timeout timer2-timeout timer3-timeout]<br><br><b>Example:</b><br>Router(config-if)# atm mcpt-timers 100 200 250                                              | Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet. <ul style="list-style-type: none"> <li>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</li> <li>The respective default values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> </li> <li>You can specify either the number of microseconds or use the default.</li> <li>The respective range of values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> </li> </ul> |
| <b>Step 10</b> | <b>no shutdown</b><br><br><b>Example:</b><br>Router(config-if)# no shutdown                                                                                                                 | Enables the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 11</b> | <b>class-int</b> <i>vc-class-name</i><br><br><b>Example:</b><br>Router(config-if)# class-int cellpacking                                                                                    | Applies a VC class to the ATM main interface or subinterface.<br><br><b>Note</b> You can also apply a VC class to a PVC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 12</b> | <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i> <b>l2transport</b><br><br><b>Example:</b><br>Router(config-if)# pvc 1/200 l2transport                                                             | Creates or assigns a name to an ATM PVC and enters L2transport VC configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVC is a switched PVC instead of a terminated PVC.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 13</b> | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> <b>encapsulation</b> <b>mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvc)# xconnect 10.13.13.13 100 encapsulation mpls | Binds the attachment circuit to a pseudowire VC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Configuring ATM Packed Cell Relay over MPLS in VP Mode

Perform this task to configure the ATM cell-packing feature in VP mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm $\textit{slot}$ /port**
4. **shutdown**
5. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
6. **no shutdown**
7. **atm pvp vpi l2transport**
8. **xconnect peer-router-id vcid encapsulation mpls**
9. **cell-packing** [*cells*] [**mcpt-timer** *timer*]

### DETAILED STEPS

|        | Command or Action                                                                                              | Purpose                                                                                                               |
|--------|----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                 | Enters global configuration mode.                                                                                     |
| Step 3 | <b>interface atm<math>\textit{slot}</math>/port</b><br><br><b>Example:</b><br>Router(config)# interface atml/0 | Defines the interface and enters interface configuration mode.                                                        |
| Step 4 | <b>shutdown</b><br><br><b>Example:</b><br>Router(config-if)# shutdown                                          | Shuts down the interface.                                                                                             |

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>atm mcpt-timers</b> [timer1-timeout timer2-timeout timer3-timeout]</p> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p>            | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <ul style="list-style-type: none"> <li>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</li> <li>The respective default values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> </li> <li>You can specify either the number of microseconds or use the default.</li> <li>The respective range of values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> </li> </ul> |
| Step 6 | <p><b>no shutdown</b></p> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                               | Enables the interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 7 | <p><b>atm pvp vpi l2transport</b></p> <p><b>Example:</b><br/>Router(config-if)# atm pvp 1 l2transport</p>                                                         | <p>Specifies that the PVP is dedicated to transporting ATM cells and enters L2transport PVP configuration submode.</p> <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVP is for cell relay. This submode is for Layer 2 transport only; it is not for regular PVPs.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 8 | <p><b>xconnect</b> peer-router-id vcid encapsulation mpls</p> <p><b>Example:</b><br/>Router(cfg-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls</p> | <p>Binds the attachment circuit to a pseudowire VC.</p> <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 9 | <p><b>cell-packing</b> [cells] [mcpt-timer timer]</p> <p><b>Example:</b><br/>Router(cfg-if-atm-l2trans-pvp)# cell-packing 10 mcpt-timer 1</p>                     | <p>Enables cell packing and specifies the cell-packing parameters.</p> <ul style="list-style-type: none"> <li>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.</li> <li>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.</li> <li>See the <b>cell-packing</b> command page for more information.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Configuring ATM Packed Cell Relay over MPLS in Port Mode

Perform this task to configure ATM packed cell relay over MPLS in port mode.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *atmslot/port*
4. **shutdown**
5. **atm mcpt-timers** [*timer1-timeout timer2-timeout timer3-timeout*]
6. **no shutdown**
7. **cell-packing** [*cells*] [**mcpt-timer** *timer*]
8. **xconnect** *peer-router-id vcid encapsulation mpls*
9. **exit**
10. **exit**
11. **show atm cell-packing**
12. **show atm vp**

### DETAILED STEPS

|        | Command or Action                                                                               | Purpose                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                  | Enters global configuration mode.                                                                                   |
| Step 3 | <b>interface</b> <i>atmslot/port</i><br><br><b>Example:</b><br>Router(config)# interface atm1/0 | Specifies an ATM interface and enters interface configuration mode.                                                 |
| Step 4 | <b>shutdown</b><br><br><b>Example:</b><br>Router(config-if)# shutdown                           | Shuts down the interface.                                                                                           |

|               |                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <pre>atm mcpt-timers [timer1-timeout timer2-timeout timer3-timeout]</pre> <p><b>Example:</b><br/>Router(config-if)# atm mcpt-timers 100 200 250</p>   | <p>Sets up the cell-packing timers, which specify how long the PE router can wait for cells to be packed into an MPLS packet.</p> <ul style="list-style-type: none"> <li>You can set up to three timers. For each timer, you specify the MCPT. This value gives the cell-packing function a limited amount of time to complete. If the timer expires before the maximum number of cells are packed into an AToM packet, the packet is sent anyway. The timeout's default and range of acceptable values depends on the ATM link speed.</li> <li>The respective default values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 30, 60, and 90 microseconds</li> <li>T3: 100, 200, and 300 microseconds</li> <li>E3: 130, 260, and 390 microseconds</li> </ul> </li> <li>You can specify either the number of microseconds or use the default.</li> <li>The respective range of values for the PA-A3 port adapters are: <ul style="list-style-type: none"> <li>OC-3: 10 to 4095 microseconds</li> <li>T3: 30 to 4095 microseconds</li> <li>E3: 40 to 4095 microseconds</li> </ul> </li> </ul> |
| <b>Step 6</b> | <pre>no shutdown</pre> <p><b>Example:</b><br/>Router(config-if)# no shutdown</p>                                                                      | <p>Enables the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 7</b> | <pre>cell-packing [cells] [mcpt-timer timer]</pre> <p><b>Example:</b><br/>Router(config-if)# cell-packing 10 mcpt-timer 1</p>                         | <p>Enables cell packing and specifies the cell-packing parameters.</p> <ul style="list-style-type: none"> <li>The <i>cells</i> argument represents the maximum number of cells to be packed into an MPLS packet. The range is from 2 to the MTU of the interface divided by 52. The default is MTU/52.</li> <li>The <i>timer</i> argument allows you to specify which timer to use. The default is timer 1.</li> <li>See the cell-packing command page for more information.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 8</b> | <pre>xconnect peer-router-id vcid encapsulation mpls</pre> <p><b>Example:</b><br/>Router(config-if)# xconnect 10.0.0.1 123<br/>encapsulation mpls</p> | <p>Binds the attachment circuit to the interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 9</b> | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-if)# exit</p>                                                                                    | <p>Exits interface configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                |                                                  |                                    |
|----------------|--------------------------------------------------|------------------------------------|
| <b>Step 10</b> | <b>exit</b>                                      | Exits global configuration mode.   |
|                | <b>Example:</b><br>Router(config)# exit          |                                    |
| <b>Step 11</b> | <b>show atm cell-packing</b>                     | Displays cell-packing statistics.  |
|                | <b>Example:</b><br>Router# show atm cell-packing |                                    |
| <b>Step 12</b> | <b>show atm vp</b>                               | Displays cell-packing information. |
|                | <b>Example:</b><br>Router#show atm vp            |                                    |

## Examples

The **show atm cell-packing** command in the following example displays the following statistics:

- The number of cells that are to be packed into an MPLS packet on the local and peer routers
- The average number of cells sent and received
- The timer values associated with the local router

Router# **show atm cell-packing**

|                  | circuit | local | average                         | peer | average                              | MCPT |
|------------------|---------|-------|---------------------------------|------|--------------------------------------|------|
|                  | type    | MNCP  | nbr of cells<br>rcvd in one pkt | MNCP | nbr of cells<br>sent in one pkt (us) |      |
| atm 1/0 vc 1/200 | 20      | 15    | 30                              | 20   | 60                                   |      |
| atm 1/0 vp 2     | 25      | 21    | 30                              | 24   | 100                                  |      |

The **show atm vp** command in the following example displays the cell packing information at the end of the output:

Router# **show atm vp 12**

ATM5/0 VPI: 12, Cell Relay, PeakRate: 149760, CesRate: 0, DataVCs: 1, CesVCs: 0, Status: ACTIVE

| VCD | VCI | Type | InPkts | OutPkts | AAL/Encap | Status |
|-----|-----|------|--------|---------|-----------|--------|
| 6   | 3   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |
| 7   | 4   | PVC  | 0      | 0       | F4 OAM    | ACTIVE |

TotalInPkts: 0, TotalOutPkts: 0, TotalInFast: 0, TotalOutFast: 0,  
 TotalBroadcasts: 0 TotalInPktDrops: 0, TotalOutPktDrops: 0  
 Local MNCP: 5, average number of cells received: 3  
 Peer MNCP: 1, average number of cells sent: 1  
 Local MCPT: 100 us

## Troubleshooting Tips

To debug ATM cell packing, issue the **debug atm cell-packing** command.

## Configuring Ethernet over MPLS in VLAN Mode

A VLAN is a switched network that is logically segmented by functions, project teams, or applications regardless of the physical location of users. Ethernet over MPLS allows you to connect two VLAN networks that are in different locations. You configure the PE routers at each end of the MPLS backbone and add a point-to-point VC. Only the two PE routers at the ingress and egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 VLAN traffic. All other routers do not have table entries for those VCs. Ethernet over MPLS in VLAN mode transports Ethernet traffic from a source 802.1Q VLAN to a destination 802.1Q VLAN over a core MPLS network.



### Note

You must configure Ethernet over MPLS (VLAN mode) on the subinterfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/interface.subinterface*
4. **encapsulation dot1q** *vlan-id*
5. **xconnect** *peer-router-id vcid encapsulation mpls*

### DETAILED STEPS

|        | Command or Action                                                                                                                               | Purpose                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                  | Enters global configuration mode.                                                                                                                                                                                                        |
| Step 3 | <b>interface gigabitethernet</b><br><i>slot/interface.subinterface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0.1 | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode. <ul style="list-style-type: none"> <li>• Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.</li> </ul> |

|               |                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                       |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <code>encapsulation dot1q <i>vlan-id</i></code><br><br><b>Example:</b><br>Router(config-subif)# <code>encapsulation dot1q 100</code>                                                             | Enables the subinterface to accept 802.1Q VLAN packets.<br><br><ul style="list-style-type: none"> <li>The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers do not.</li> </ul> |
| <b>Step 5</b> | <code>xconnect <i>peer-router-id</i> <i>vcid</i> encapsulation mpls</code><br><br><b>Example:</b><br>Router(config-subif)# <code>xconnect 10.0.0.1 123</code><br><code>encapsulation mpls</code> | Binds the attachment circuit to a pseudowire VC.<br><br><ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                                                                                                |

## Configuring Ethernet over MPLS in Port Mode

Port mode allows a frame coming into an interface to be packed into an MPLS packet and transported over the MPLS backbone to an egress interface. The entire Ethernet frame without the preamble or FCS is transported as a single packet. To configure port mode, you use the **xconnect** command in interface configuration mode and specify the destination address and the VC ID. The syntax of the **xconnect** command is the same as for all other transport types. Each interface is associated with one unique pseudowire VC label.

When configuring Ethernet over MPLS in port mode, use the following guidelines:

- The pseudowire VC type is set to Ethernet.
- Port mode and Ethernet VLAN mode are mutually exclusive. If you enable a main interface for port-to-port transport, you cannot also enter commands on a subinterface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *gigabitethernet**slot*/*interface***
4. **xconnect *peer-router-id* *vcid* encapsulation mpls**
5. **exit**
6. **exit**
7. **show mpls l2transport vc**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                    | Purpose                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                       | Enters global configuration mode.                                                                                                                                                                                             |
| Step 3 | <b>interface gigabitethernet</b> <i>slot/interface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0                                        | Specifies the Gigabit Ethernet interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>Make sure the interface on the adjoining CE router is on the same VLAN as this PE router.</li> </ul> |
| Step 4 | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i><br><b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                                               |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                        | Exits interface configuration mode.                                                                                                                                                                                           |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                           | Exits router configuration mode.                                                                                                                                                                                              |
| Step 7 | <b>show mpls l2transport vc</b><br><br><b>Example:</b><br>Router# show mpls l2transport vc                                                                           | Displays information about Ethernet over MPLS port mode.                                                                                                                                                                      |

## Examples

In the following example, the output of the **show mpls l2transport vc detail** command is displayed:

```
Router# show mpls l2transport vc detail
```

```
Local interface: Gi4/0.1 up, line protocol up, Eth VLAN 2 up
Destination address: 10.1.1.1, VC ID: 2, VC status: up
.
.
.
Local interface: Gi8/0/1 up, line protocol up, Ethernet up
Destination address: 10.1.1.1, VC ID: 8, VC status: up
```

## Configuring Ethernet over MPLS with VLAN ID Rewrite

The VLAN ID rewrite feature enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel.

The Cisco 12000 series router requires you to configure VLAN ID rewrite manually, as described in the following sections.

The following routers automatically perform VLAN ID rewrite on the disposition PE router. No configuration is required:

- Cisco 7200 series routers.
- Cisco 7500 series routers.
- Cisco 10720 series routers.
- Routers supported on Cisco IOS Release 12.4(11)T. (Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support.)

The following sections explain how to configure the VLAN ID rewrite feature:

- [Guidelines for Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0\(29\)S and Earlier Releases, page 48](#)
- [Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0\(30\)S and Later Releases, page 49](#)

### Guidelines for Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0(29)S and Earlier Releases

Use the following guidelines for the VLAN ID rewrite feature for the Cisco 12000 series routers in Cisco IOS releases earlier than 12.0(29)S:

- The IP Service Engine (ISE) 4-port Gigabit Ethernet line card performs the VLAN ID rewrite on the disposition side at the edge-facing line card.
- The engine 2 3-port Gigabit Ethernet line card performs the VLAN ID rewrite on the imposition side at the edge-facing line card.

The VLAN ID rewrite functionality requires that both ends of the Ethernet over MPLS connections be provisioned with the same line cards. Make sure that both edge-facing ends of the virtual circuit use either the engine 2 or ISE Ethernet line card. The following example shows the system flow with the VLAN ID rewrite feature:

- The ISE 4-port Gigabit Ethernet line card:  
Traffic flows from VLAN1 on CE1 to VLAN2 on CE2. As the frame reaches the edge-facing line card of the disposition router PE2, the VLAN ID in the dot1Q header changes to the VLAN ID assigned to VLAN2.
- The engine 2 3-port Gigabit Ethernet line card:  
Traffic flows from VLAN1 on CE1 to VLAN2 on CE2. As the frame reaches the edge-facing line card of the imposition router PE1, the VLAN ID in the dot1Q header changes to the VLAN ID assigned to VLAN2.

For the Cisco 12000 series router engine 2 3-port Gigabit Ethernet line card, you must issue the **remote circuit id** command as part of the Ethernet over MPLS VLAN ID rewrite configuration.

## Configuring Ethernet over MPLS with VLAN ID Rewrite for the Cisco 12000 Series Routers for Cisco IOS Releases 12.0(30)S and Later Releases

In Cisco IOS Release 12.0(30)S, the following changes to VLAN ID rewrite were implemented:

- The ISE 4-port Gigabit Ethernet line card can perform VLAN ID rewrite at both the imposition and disposition sides of the edge-facing router.
- The **remote circuit id** command is not required as part of the Ethernet over MPLS VLAN ID rewrite configuration, as long as both PE routers are running Cisco IOS Release 12.0(30)S. The VLAN ID rewrite feature is implemented automatically when you configure Ethernet over MPLS.
- The VLAN ID rewrite feature in Cisco IOS Release 12.0(30)S can interoperate with routers that are running earlier releases. If you have a PE router at one end of the circuit that is using an earlier Cisco IOS release and the **remote circuit id** command, the other PE can run Cisco IOS Release 12.0(30)S and still perform VLAN ID rewrite.
- You can mix the line cards on the PE routers, as shown in the following table

**Table 6** Supported Line Cards for VLAN ID Rewrite Feature:

| If PE1 Has These Line Cards                                                               | Then PE2 Can Use These Line Cards                                                         |
|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Engine 2 3-port Gigabit Ethernet line card<br>or<br>ISE 4-port Gigabit Ethernet line card | Engine 2 3-port Gigabit Ethernet line card<br>or<br>ISE 4-port Gigabit Ethernet line card |
| ISE 4-port Gigabit Ethernet line card                                                     | Any Cisco 12000 series router line card                                                   |

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet** *slot/port.subinterface*
4. **encapsulation dot1q** *vlan-id*
5. **xconnect** *peer-router-id vcid encapsulation mpls*
6. **remote circuit id** *remote-vlan-id*
7. **exit**
8. **exit**
9. **exit**
10. **show controllers eompls forwarding-table**

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>interface</b><br><b>gigabitethernet</b> <i>slot/interface.subinterface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0.1 | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode. <ul style="list-style-type: none"> <li>Make sure the subinterfaces between the CE and PE routers that are running Ethernet over MPLS are in the same subnet. All other subinterfaces and backbone routers do not need to be in the same subnet.</li> </ul> |
| Step 4 | <b>encapsulation dot1q</b> <i>vlan-id</i><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                      | Enables the subinterface to accept 802.1Q VLAN packets. <ul style="list-style-type: none"> <li>Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.</li> </ul>                                                                                                                                             |
| Step 5 | <b>xconnect</b> <i>peer-router-id vcid encapsulation mpls</i><br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC and enters xconnect configuration mode. <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                                                                                                                             |
| Step 6 | <b>remote circuit id</b> <i>remote-vlan-id</i><br><br><b>Example:</b><br>Router(config-subif-xconn)# remote circuit id 101                             | Enables you to use VLAN interfaces with different VLAN IDs at both ends of the tunnel. <ul style="list-style-type: none"> <li>This command is required only for the Cisco 12000 series router engine 2 3-port Gigabit Ethernet line card.</li> </ul>                                                                                               |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-subif-xconn)# exit                                                                                 | Exits xconnect configuration mode.                                                                                                                                                                                                                                                                                                                 |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-subif)# exit                                                                                       | Exits subinterface configuration mode.                                                                                                                                                                                                                                                                                                             |

|                |                                                                                                                                           |                                             |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                | Exits global configuration mode.            |
| <b>Step 10</b> | <b>show controllers eompls forwarding-table</b><br><br><b>Example:</b><br>Router# execute slot 0 show controllers eompls forwarding-table | Displays information about VLAN ID rewrite. |

## Examples

The command output of the **show controllers eompls forwarding-table** command in the following example shows VLAN ID rewrite configured on the Cisco 12000 series routers with an engine 2 3-port Gigabit Ethernet line card. In the following example, the bolded command output show the VLAN ID rewrite information.

### On PE1

```
Router# execute slot 0 show controllers eompls forwarding-table 0 2
```

```
Port # 0, VLAN-ID # 2, Table-index 2
EoMPLS configured: 1
tag_rew_ptr          = D001BB58
Leaf entry?          = 1
FCR index             = 20
    **tagrew_psa_addr   = 0006ED60
    **tagrew_vir_addr   = 7006ED60
    **tagrew_phy_addr   = F006ED60
[0-7] loq 8800 mtu 4458 oq 4000 ai 3 oi 04019110 (encaps size 4)
cw-size 4 vlanid-rew 3
gather A30 (bufhdr size 32 EoMPLS (Control Word) Imposition profile 81)
2 tag: 18 18
counters 1182, 10 reported 1182, 10.
Local OutputQ (Unicast): Slot:2 Port:0 RED queue:0 COS queue:0
Output Q (Unicast):      Port:0 RED queue:0 COS queue:0
```

### On PE2

```
Router# execute slot 0 show controllers eompls forwarding-table 0 3
```

```
Port # 0, VLAN-ID # 3, Table-index 3
EoMPLS configured: 1
tag_rew_ptr          = D0027B90
Leaf entry?          = 1
FCR index             = 20
    **tagrew_psa_addr   = 0009EE40
    **tagrew_vir_addr   = 7009EE40
    **tagrew_phy_addr   = F009EE40
[0-7] loq 9400 mtu 4458 oq 4000 ai 8 oi 84000002 (encaps size 4)
cw-size 4 vlanid-rew 2
gather A30 (bufhdr size 32 EoMPLS (Control Word) Imposition profile 81)
2 tag: 17 18
counters 1182, 10 reported 1182, 10.
Local OutputQ (Unicast): Slot:5 Port:0 RED queue:0 COS queue:0
Output Q (Unicast):      Port:0 RED queue:0 COS queue:0
```

## Configuring per-Subinterface MTU for Ethernet over MPLS

Cisco IOS Release 12.2(33)SRC introduces the ability to specify MTU values in xconnect subinterface configuration mode. When you use xconnect subinterface configuration mode to set the MTU value, you establish a pseudowire connection for situations where the interfaces have different MTU values that cannot be changed.

If you specify an MTU value in xconnect subinterface configuration mode that is outside the range of supported MTU values (64 bytes to the maximum number of bytes supported by the interface), the command might be rejected. If you specify an MTU value that is out of range in xconnect subinterface configuration mode, the router enters the command in subinterface configuration mode.

### Restrictions

Configuring the MTU value in xconnect subinterface configuration mode has the following restrictions:

- The following features do not support MTU values in xconnect subinterface configuration mode:
  - Layer 2 Tunnel Protocol Version 3 (L2TPv3)
  - Virtual Private LAN services (VPLS)
  - L2VPN Pseudowire Switching
- The MTU value can be configured in xconnect subinterface configuration mode only on the following interfaces and subinterfaces:
  - Ethernet
  - FastEthernet
  - Gigabit Ethernet
- The router uses an MTU validation process for remote VCs established through LDP, which compares the MTU value configured in xconnect subinterface configuration mode to the MTU value of the remote customer interface. If an MTU value has not been configured in xconnect subinterface configuration mode, then the validation process compares the MTU value of the local customer interface to the MTU value of the remote xconnect, either explicitly configured or inherited from the underlying interface or subinterface.
- When you configure the MTU value in xconnect subinterface configuration mode, the specified MTU value is not enforced by the dataplane. The dataplane enforces the MTU values of the interface (port mode) or subinterface (VLAN mode).
- Ensure that the interface MTU is larger than the MTU value configured in xconnect subinterface configuration mode. If the MTU value of the customer-facing subinterface is larger than the MTU value of the core-facing interface, traffic may not be able to travel across the pseudowire.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface gigabitethernet *slot/interface***
4. **mtu *mtu-value***
5. **interface gigabitethernet *slot/interface.subinterface***
6. **encapsulation dot1q *vlan-id***
7. **xconnect *peer-router-id vcid* encapsulation mpls**

8. **mtu** *mtu-value*
9. **end**
10. **show mpls l2transport binding**

## DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                   |
| Step 3 | <b>interface gigabitethernet</b> <i>slot/interface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet4/0                                 | Specifies the Gigabit Ethernet interface and enters interface configuration mode.                                                                                                                                                                                                   |
| Step 4 | <b>mtu</b> <i>mtu-value</i><br><br><b>Example:</b><br>Router(config-if)# mtu 2000                                                                             | Specifies the MTU value for the interface. <ul style="list-style-type: none"> <li>The MTU value specified at the interface level can be inherited by a subinterface.</li> </ul>                                                                                                     |
| Step 5 | <b>interface gigabitethernet</b> <i>slot</i><br><i>/interface.subinterface</i><br><br><b>Example:</b><br>Router(config-if)# interface<br>gigabitethernet4/0.1 | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode. <ul style="list-style-type: none"> <li>Make sure the subinterface on the adjoining CE router is on the same VLAN as this PE router.</li> </ul>                                              |
| Step 6 | <b>encapsulation dot1q</b> <i>vlan-id</i><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                             | Enables the subinterface to accept 802.1Q VLAN packets. <ul style="list-style-type: none"> <li>The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers need not be.</li> </ul> |
| Step 7 | <b>xconnect</b> <i>peer-router-id vcid encapsulation mpls</i><br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123<br>encapsulation mpls     | Binds the attachment circuit to a pseudowire VC. <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports. Enters xconnect subinterface configuration mode.</li> </ul>                                                    |
| Step 8 | <b>mtu</b> <i>mtu-value</i><br><br><b>Example:</b><br>Router(config-if-xconn)# mtu 1400                                                                       | Specifies the MTU for the VC.                                                                                                                                                                                                                                                       |

|         | Command or Action                                                                                    | Purpose                                                                                  |
|---------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Step 9  | <b>end</b><br><br><b>Example:</b><br>Router(config-if-xconn)# end                                    | Exits xconnect subinterface configuration mode and returns to global configuration mode. |
| Step 10 | <b>show mpls l2transport binding</b><br><br><b>Example:</b><br>Router# show mpls l2transport binding | Displays the MTU values assigned to the local and remote interfaces.                     |

## Configuring Frame Relay over MPLS with DLCI-to-DLCI Connections

Frame Relay over MPLS encapsulates Frame Relay PDUs in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up data-link connection identifier (DLCI)-to-DLCI connections or port-to-port connections. With DLCI-to-DLCI connections, the PE routers manipulate the packet by removing headers, adding labels, and copying control word elements from the header to the PDU.

Perform this task to configure Frame Relay over MPLS with DLCI-to-DLCI connections.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **frame-relay switching**
4. **interface serialslot/port**
5. **encapsulation frame-relay [cisco / ietf]**
6. **frame-relay intf-type dce**
7. **exit**
8. **connect connection-name interface dlci l2transport**
9. **xconnect peer-router-id vcid encapsulation mpls**

### DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                            |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                  |



|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>frame-relay switching</b><br><br><b>Example:</b><br>Router(config)# frame-relay switching                                                                        | Enables PVC switching on a Frame Relay device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 4 | <b>interface serialslot/port</b><br><br><b>Example:</b><br>Router(config)# interface serial3/1                                                                      | Specifies a serial interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>encapsulation frame-relay [cisco   ietf]</b><br><br><b>Example:</b><br>Router(config-if)# encapsulation frame-relay ietf                                         | Specifies Frame Relay encapsulation for the interface. <ul style="list-style-type: none"> <li>You can specify different types of encapsulations. You can set one interface to Cisco encapsulation and the other interface to IETF encapsulation.</li> </ul>                                                                                                                                                                                                                                                                                                         |
| Step 6 | <b>frame-relay intf-type dce</b><br><br><b>Example:</b><br>Router(config-if)# frame-relay intf-type dce                                                             | Specifies that the interface is a DCE switch. <ul style="list-style-type: none"> <li>You can also specify the interface to support Network-to-Network Interface (NNI) and DTE connections.</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                                                       | Exits from interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 8 | <b>connect connection-name interface dlci</b><br><b>l2transport</b><br><br><b>Example:</b><br>Router(config)# connect fr1 serial5/0 1000 l2transport                | Defines connections between Frame Relay PVCs and enters connect configuration submode. <ul style="list-style-type: none"> <li>Using the <b>l2transport</b> keyword specifies that the PVC will not be a locally switched PVC, but will be tunneled over the backbone network.</li> <li>The <i>connection-name</i> argument is a text string that you provide.</li> <li>The <i>interface</i> argument is the interface on which a PVC connection will be defined.</li> <li>The <i>dlci</i> argument is the DLCI number of the PVC that will be connected.</li> </ul> |
| Step 9 | <b>xconnect peer-router-id vcid</b><br><b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-fr-pw-switching)# xconnect 10.0.0.1 123 encapsulation mpls | Creates the VC to transport the Layer 2 packets. <ul style="list-style-type: none"> <li>In a DLCI-to-DLCI connection type, Frame Relay over MPLS uses the <b>xconnect</b> command in connect configuration submode.</li> </ul>                                                                                                                                                                                                                                                                                                                                      |

## Configuring Frame Relay over MPLS with Port-to-Port Connections

Frame Relay over MPLS encapsulates Frame Relay PDUs in MPLS packets and forwards them across the MPLS network. For Frame Relay, you can set up DLCI-to-DLCI connections or port-to-port connections. With port-to-port connections, you use HDLC mode to transport the Frame Relay

encapsulated packets. In HDLC mode, the whole HDLC packet is transported. Only the HDLC flags and FCS bits are removed. The contents of the packet are not used or changed, including the backward explicit congestion notification (BECN), forward explicit congestion notification (FECN) and discard eligibility (DE) bits.

Perform this task to set up Frame Relay port-to-port connections.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serial***slot/port*
4. **encapsulation hdlc**
5. **xconnect** *peer-router-id vcid encapsulation mpls*

## DETAILED STEPS

|        | Command or Action                                                                                                                                   | Purpose                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                      | Enters global configuration mode.                                                                                  |
| Step 3 | <b>interface serial</b> <i>slot/port</i><br><br><b>Example:</b><br>Router(config)# interface serial5/0                                              | Specifies a serial interface and enters interface configuration mode.                                              |
| Step 4 | <b>encapsulation hdlc</b><br><br><b>Example:</b><br>Router(config-if)# encapsulation hdlc                                                           | Specifies that Frame Relay PDUs will be encapsulated in HDLC packets.                                              |
| Step 5 | <b>xconnect</b> <i>peer-router-id vcid encapsulation mpls</i><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 encapsulation mpls | Creates the VC to transport the Layer 2 packets.                                                                   |

## Configuring HDLC and PPP over MPLS

With HDLC over MPLS, the whole HDLC packet is transported. The ingress PE router removes only the HDLC flags and FCS bits. The contents of the packet are not used or changed.

With PPP over MPLS, the ingress PE router removes the flags, address, control field, and the FCS.

## Restrictions

The following restrictions pertain to the HDLC over MPLS feature:

- Asynchronous interfaces are not supported.
- You must configure HDLC over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces.

The following restrictions pertain to the PPP over MPLS feature:

- Zero hops on one router is not supported. However, you can have back-to-back PE routers.
- Asynchronous interfaces are not supported. The connections between the CE and PE routers on both ends of the backbone must have similar link layer characteristics. The connections between the CE and PE routers must both be synchronous.
- Multilink PPP (MLP) is not supported.
- You must configure PPP on router interfaces only. You cannot configure PPP on subinterfaces.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface serialslot/port**
4. **encapsulation encapsulation-type**
5. **xconnect peer-router-id vcid encapsulation mpls**

## DETAILED STEPS

|        | Command or Action                                                                              | Purpose                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                 | Enters global configuration mode.                                                                                                                                                                                                                    |
| Step 3 | <b>interface serialslot/port</b><br><br><b>Example:</b><br>Router(config)# interface serial5/0 | Specifies a serial interface and enters interface configuration mode. <ul style="list-style-type: none"> <li>• You must configure HDLC and PPP over MPLS on router interfaces only. You cannot configure HDLC over MPLS on subinterfaces.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                      | Purpose                                                                    |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Step 4 | <code>encapsulation ppp</code><br>or<br><code>encapsulation hdlc</code><br><br><b>Example:</b><br>Router(config-if)# <code>encapsulation ppp</code><br>or<br><br><b>Example:</b><br>Router(config-if)# <code>encapsulation hdlc</code> | Specifies HDLC or PPP encapsulation and enters connect configuration mode. |
| Step 5 | <code>xconnect peer-router-id vcid</code><br><code>encapsulation mpls</code><br><br><b>Example:</b><br>Router(config-fr-pw-switching)# <code>xconnect 10.0.0.1 123 encapsulation mpls</code>                                           | Creates the VC to transport the Layer 2 packets.                           |

## Configuring Tunnel Selection

The tunnel selection feature allows you to specify the path that traffic uses. You can specify either an MPLS TE tunnel or destination IP address or domain name server (DNS) name.

You also have the option of specifying whether the VCs should use the default path (the path LDP uses for signaling) if the preferred path is unreachable. This option is enabled by default; you must explicitly disable it.

You configure tunnel selection when you set up the pseudowire class. You enable tunnel selection with the **preferred-path** command. Then, you apply the pseudowire class to an interface that has been configured to transport AToM packets.

The following guidelines provide more information about configuring tunnel selection:

- The **preferred-path** command is available only if the pseudowire encapsulation type is MPLS.
- This tunnel selection feature is enabled when you exit from pseudowire submode.
- The selected path should be an LSP destined to the peer PE router.
- The selected tunnel must be an MPLS TE tunnel.
- If you select a tunnel, the tunnel tailend must be on the remote PE router.
- If you specify an IP address, that address must be the IP address of the loopback interface on the remote PE router. The address must have a /32 mask. There must be an LSP destined to that selected address. The LSP need not be a TE tunnel.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**

5. **preferred-path** {**interface tunnel** *tunnel-number* | **peer** {*ip-address* / *host-name*}} [**disable-fallback**]
6. **exit**
7. **interface** *slot/port*
8. **encapsulation** *encapsulation-type*
9. **xconnect** *peer-router-id* *vcid* **pw-class** *name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                              | Purpose                                                                                                                                   |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                 | Enters global configuration mode.                                                                                                         |
| Step 3 | <b>pseudowire-class</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# pseudowire-class ts1                                                                                                                                             | Establishes a pseudowire class with a name that you specify and enters pseudowire configuration mode.                                     |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw-class)#<br>encapsulation mpls                                                                                                                                             | Specifies the tunneling encapsulation. <ul style="list-style-type: none"> <li>For AToM, the encapsulation type is <b>mpls</b>.</li> </ul> |
| Step 5 | <b>preferred-path</b> { <b>interface tunnel</b> <i>tunnel-number</i>   <b>peer</b> { <i>ip-address</i>   <i>host-name</i> }} [ <b>disable-fallback</b> ]<br><br><b>Example:</b><br>Router(config-pw-class)# preferred<br>path peer 10.18.18.18 | Specifies the MPLS traffic engineering tunnel or IP address or hostname to be used as the preferred path.                                 |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pw-class)# exit                                                                                                                                                                            | Exits from pseudowire configuration mode.                                                                                                 |
| Step 7 | <b>interface</b> <i>slot/port</i><br><br><b>Example:</b><br>Router(config)# interface atml1/1                                                                                                                                                  | Specifies an interface and enters interface configuration mode.                                                                           |

|        | Command or Action                                                                                                                        | Purpose                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------|
| Step 8 | <b>encapsulation</b> <i>encapsulation-type</i><br><br><b>Example:</b><br>Router(config-if)# encapsulation aal5                           | Specifies the encapsulation for the interface.   |
| Step 9 | <b>xconnect</b> <i>peer-router-id vcid pw-class name</i><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.0.0.1 123 pw-class tsl | Binds the attachment circuit to a pseudowire VC. |

## Examples

In the following example, the **show mpls l2transport vc** command shows the following information about the VCs:

- VC 101 has been assigned a preferred path called Tunnel1. The default path is disabled, because the preferred path specified that the default path should not be used if the preferred path fails.
- VC 150 has been assigned an IP address of a loopback address on PE2. The default path can be used if the preferred path fails.

In the following example, command output that is bolded shows the preferred path information.

Router# **show mpls l2transport vc detail**

```
Local interface: Gi0/0/0.1 up, line protocol up, Eth VLAN 222 up
  Destination address: 10.16.16.16, VC ID: 101, VC status: up
    Preferred path: Tunnel1, active
    Default path: disabled
    Tunnel label: 3, next hop point2point
    Output interface: Tu1, imposed label stack {17 16}
  Create time: 00:27:31, last status change time: 00:27:31
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 25, remote 16
    Group ID: local 0, remote 6
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 10, send 10
    byte totals:   receive 1260, send 1300
    packet drops:  receive 0, send 0
```

```
Local interface: AT1/0/0 up, line protocol up, ATM AAL5 0/50 up
  Destination address: 10.16.16.16, VC ID: 150, VC status: up
    Preferred path: 10.18.18.18, active
    Default path: ready
    Tunnel label: 3, next hop point2point
    Output interface: Tu2, imposed label stack {18 24}
  Create time: 00:15:08, last status change time: 00:07:37
  Signaling protocol: LDP, peer 10.16.16.16:0 up
    MPLS VC labels: local 26, remote 24
    Group ID: local 2, remote 0
    MTU: local 4470, remote 4470
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
```

```
packet totals: receive 0, send 0
byte totals:   receive 0, send 0
packet drops:  receive 0, send 0
```

## Troubleshooting Tips

You can use the **debug mpls l2transport vc event** command to troubleshoot tunnel selection. For example, if the tunnel interface that is used for the preferred path is shut down, the default path is enabled. The **debug mpls l2transport vc event** command provides the following output:

```
AToM SMGR [10.2.2.2, 101]: Processing imposition update, vc_handle 62091860, update_action
3, remote_vc_label 16
AToM SMGR [10.2.2.2, 101]: selected route no parent rewrite: tunnel not up
AToM SMGR [10.2.2.2, 101]: Imposition Programmed, Output Interface: Et3/2
```

## Setting Experimental Bits with AToM

MPLS AToM uses the three experimental bits in a label to determine the queue of packets. You statically set the experimental bits in both the VC label and the LSP tunnel label, because the LSP tunnel label might be removed at the penultimate router. The following sections explain the transport-specific implementations of the EXP bits.



### Note

For information about setting EXP bits on the Cisco 12000 series router for Cisco IOS Release 12.0(30)S, see the *AToM: L2 QoS* feature module.

For configuration steps and examples, see the [“Setting Experimental Bits with AToM” section on page 61](#).

## Restrictions

The following restrictions apply to ATM AAL5 over MPLS with EXP bits:

- ATM AAL5 over MPLS allows you to statically set the experimental bits.
- If you do not assign values to the experimental bits, the priority bits in the header’s “tag control information” field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to ATM Cell Relay over MPLS with EXP bits:

- ATM Cell Relay over MPLS allows you to statically set the experimental bits in VC, PVP, and port modes.
- If you do not assign values to the experimental bits, the priority bits in the header’s “tag control information” field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to Ethernet over MPLS with EXP bits:

### On the Cisco 7200 and 7500 Series Routers

- Ethernet over MPLS allows you to set the EXP bits by using either of the following methods:

- Writing the priority bits into the experimental bit field, which is the default.
- Using the **match any** command with the **set mpls exp** command.
- If you do not assign values to the experimental bits, the priority bits in the 802.1Q header's "tag control information" field are written into the experimental bit fields.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

#### On the Cisco 10720 Internet Router

Table 7 lists the commands that are supported on the Cisco 10720 Internet router for Ethernet over MPLS. The letter Y means that the command is supported on that interface. A dash (—) means that command is not supported on that interface.



#### Note

The **match cos** command is supported only on subinterfaces, not main interfaces.

**Table 7** *Commands Supported on the Cisco 10720 Router for Ethernet over MPLS*

| Commands                         | Imposition |     | Disposition |     |
|----------------------------------|------------|-----|-------------|-----|
|                                  | In         | Out | In          | Out |
| <b>Traffic Matching Commands</b> |            |     |             |     |
| <b>match any</b>                 | Y          | Y   | Y           | Y   |
| <b>match cos</b>                 | Y          | —   | —           | —   |
| <b>match input-interface</b>     | —          | —   | Y           | Y   |
| <b>match mpls exp</b>            | —          | Y   | Y           | —   |
| <b>match qos-group</b>           | —          | Y   | —           | Y   |
| <b>Traffic Action Commands</b>   |            |     |             |     |
| <b>set cos</b>                   | —          | —   | —           | Y   |
| <b>set mpls exp</b>              | Y          | —   | —           | —   |
| <b>set qos-group</b>             | Y          | —   | Y           | —   |
| <b>set srp-priority</b>          | —          | Y   | —           | —   |

The following restrictions apply to Frame Relay over MPLS and EXP bits:

- If you do not assign values to the experimental bits, the priority bits in the header's "tag control information" field are set to zero.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding must be enabled before you set the experimental bits.

The following restrictions apply to HDLC over MPLS and PPP over MPLS and EXP bits:

- If you do not assign values to the experimental bits, zeros are written into the experimental bit fields.
- On the Cisco 7500 series routers, enable distributed Cisco Express Forwarding before setting the experimental bits.

Set the experimental bits in both the VC label and the LSP tunnel label. You set the experimental bits in the VC label, because the LSP tunnel label might be removed at the penultimate router. Perform this task to set the experimental bits.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-name*
4. **match any**
5. **exit**
6. **policy-map** *policy-name*
7. **class** *class-name*
8. **set mpls experimental** *value*
9. **exit**
10. **exit**
11. **interface** *slot/port*
12. **service-policy input** *policy-name*
13. **exit**
14. **exit**
15. **show policy-map interface** *interface-name* [**vc** [*vpi*/] *vci*] [**dlci** *dlci*] [**input** | **output**]

## DETAILED STEPS

|        | Command or Action                                                                             | Purpose                                                                                                                                                                          |
|--------|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                        | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                | Enters global configuration mode.                                                                                                                                                |
| Step 3 | <b>class-map</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config)# class-map class1 | Specifies the user-defined name of the traffic class and enters class map configuration mode.                                                                                    |
| Step 4 | <b>match any</b><br><br><b>Example:</b><br>Router(config-cmap)# match any                     | Specifies that all packets will be matched.<br><ul style="list-style-type: none"><li>• Use only the <b>any</b> keyword. Other keywords might cause unexpected results.</li></ul> |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-cmap)# exit                               | Exits class map configuration mode.                                                                                                                                              |

|         | Command or Action                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                              |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>policy-map</b> <i>policy-name</i><br><br><b>Example:</b><br>Router(config)# <b>policy-map</b> policy1                                                                                                                                     | Specifies the name of the traffic policy to configure and enters policy-map configuration mode.                                                                                                                      |
| Step 7  | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-pmap)# <b>class</b> class1                                                                                                                                            | Specifies the name of the predefined traffic that was configured with the <b>class-map</b> command and was used to classify traffic to the traffic policy specified, and enters policy-map class configuration mode. |
| Step 8  | <b>set mpls experimental</b> <i>value</i><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>set mpls experimental</b> 7                                                                                                                    | Designates the value to which the MPLS bits are set if the packets match the specified policy map.                                                                                                                   |
| Step 9  | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>exit</b>                                                                                                                                                                     | Exits policy-map class configuration mode.                                                                                                                                                                           |
| Step 10 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap)# <b>exit</b>                                                                                                                                                                       | Exits policy-map configuration mode.                                                                                                                                                                                 |
| Step 11 | <b>interface</b> <i>slot/port</i><br><br><b>Example:</b><br>Router(config)# <b>interface</b> atm4/0                                                                                                                                          | Specifies the interface and enters interface configuration mode.                                                                                                                                                     |
| Step 12 | <b>service-policy input</b> <i>policy-name</i><br><br><b>Example:</b><br>Router(config-if)# <b>service-policy input</b> policy1                                                                                                              | Attaches a traffic policy to an interface.                                                                                                                                                                           |
| Step 13 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# <b>exit</b>                                                                                                                                                                         | Exits interface configuration mode.                                                                                                                                                                                  |
| Step 14 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# <b>exit</b>                                                                                                                                                                            | Exits global configuration mode.                                                                                                                                                                                     |
| Step 15 | <b>show policy-map interface</b> <i>interface-name</i> [ <b>vc</b> [ <i>vpi</i> ]/] [ <i>vci</i> ] [ <b>dlci</b> <i>dlci</i> ] [ <b>input</b>   <b>output</b> ]<br><br><b>Example:</b><br>Router# <b>show policy-map interface</b> serial3/0 | Displays the traffic policy attached to an interface.                                                                                                                                                                |

## Setting the Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers

You can use the DE bit in the address field of a Frame Relay frame to prioritize frames in congested Frame Relay networks. The Frame Relay DE bit has only one bit and can therefore only have two settings, 0 or 1. If congestion occurs in a Frame Relay network, frames with the DE bit set to 1 are discarded before frames with the DE bit set to 0. Therefore, important traffic should have the DE bit set to 0, and less important traffic should be forwarded with the DE bit set at 1. The default DE bit setting is 0. You can change the DE bit setting to 1 with the **set fr-de** command.



### Note

The **set fr-de** command can be used only in an output service policy.

Perform this task to set the Frame Relay DE bit on the Cisco 7200 and 7500 series routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-name*
4. **class** *class-name*
5. **set fr-de**

### DETAILED STEPS

|        | Command or Action                                                                                 | Purpose                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                    | Enters global configuration mode.                                                                                                                                                                        |
| Step 3 | <b>policy-map</b> <i>policy-name</i><br><br><b>Example:</b><br>Router(config)# policy-map policy1 | Specifies the name of the traffic policy to configure and enters policy-map configuration mode.<br><ul style="list-style-type: none"><li>Names can be a maximum of 40 alphanumeric characters.</li></ul> |
| Step 4 | <b>class</b> <i>class-name</i><br><br><b>Example:</b><br>Router(config-pmap)# class class1        | Specifies the name of a predefined traffic class and enters policy-map class configuration mode.                                                                                                         |
| Step 5 | <b>set fr-de</b><br><br><b>Example:</b><br>Router(config-pmap-c)# set fr-de                       | Sets the Frame Relay DE bit setting for all packets that match the specified traffic class from 0 to 1.                                                                                                  |

## Matching the Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers

You can use the **match fr-de** command to enable frames with a DE bit setting of 1 to be considered a member of a defined class and forwarded according to the specifications set in the service policy.

Perform this task to match frames with the FR DE bit set to 1.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **match fr-de**

### DETAILED STEPS

|        | Command or Action                                                                                  | Purpose                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                             | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                     | Enters global configuration mode.                                                                                   |
| Step 3 | <b>class-map</b> <i>class-map-name</i><br><br><b>Example:</b><br>Router(config)# class-map de-bits | Specifies the name of a predefined traffic class and enters class-map configuration mode.                           |
| Step 4 | <b>match fr-de</b><br><br><b>Example:</b><br>Router(config-cmap)# match fr-de                      | Classifies all frames with the DE bit set to 1.                                                                     |

## Enabling the Control Word

You can enable the control word for dynamic and static pseudowires under a pseudowire class. Use the **control-word** command to enable, disable, or set a control word to autosense mode. If you do not enable a control word, autosense is the default mode for the control word.

Perform this task to enable a control word.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *cw\_enable*

4. **encapsulation mpls**
5. **control-word**
6. **exit**
7. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                         | Enters global configuration mode.                                                                                                         |
| Step 3 | <b>pseudowire-class cw_enable</b><br><br><b>Example:</b><br>Router(config)# pseudowire-class cw_enable | Enters pseudowire class configuration mode.                                                                                               |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw-class)# encapsulation mpls        | Specifies the tunneling encapsulation. <ul style="list-style-type: none"> <li>For AToM, the encapsulation type is <b>mpls</b>.</li> </ul> |
| Step 5 | <b>control-word</b><br><br><b>Example:</b><br>Router(config-pw-class)# control-word                    | Enables the control word.                                                                                                                 |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pw-class)# exit                                    | Exits pseudowire class configuration mode and returns to global configuration mode.                                                       |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                             | Exits global configuration mode.                                                                                                          |

## Configuration Examples for Any Transport over MPLS

This section contains the following configuration examples:

- [ATM AAL5 over MPLS: Examples, page 68](#)
- [OAM Cell Emulation for ATM AAL5 over MPLS: Examples, page 69](#)

- [ATM Cell Relay over MPLS: Examples, page 70](#)
- [ATM Single Cell Relay over MPLS: Examples, page 71e](#)
- [Ethernet over MPLS: Examples, page 72](#)
- [Configuring per-Subinterface MTU for Ethernet over MPLS: Example, page 79](#)
- [Tunnel Selection: Examples, page 72](#)
- [Setting Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers: Examples, page 74](#)
- [Matching Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers: Examples, page 75](#)
- [ATM over MPLS: Examples, page 75](#)
- [Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute: Examples, page 76](#)
- [Configuring per-Subinterface MTU for Ethernet over MPLS: Example, page 79](#)
- [Configuring MTU Values in xconnect Configuration Mode for L2VPN Interworking: Example, page 81](#)
- [Removing a Pseudowire: Examples, page 84](#)

## ATM AAL5 over MPLS: Examples

### ATM AAL5 over MPLS on PVCs

The following example enables ATM AAL5 over MPLS on an ATM PVC:

```
enable
configure terminal
interface atm1/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
```

### ATM AAL5 over MPLS in VC Class Configuration Mode

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

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0
class-int aal5class
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm aal5class
encapsulation aal5
interface atm1/0
pvc 1/200 l2transport
class-vc aal5class
xconnect 10.13.13.13 100 encapsulation mpls
```

## OAM Cell Emulation for ATM AAL5 over MPLS: Examples

### OAM Cell Emulation for ATM AAL5 over MPLS on PVCs

The following example enables OAM cell emulation on an ATM PVC:

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable
oam-pvc manage
```

The following example sets the rate at which an AIS cell is sent every 30 seconds:

```
interface ATM 1/0/0
pvc 1/200 l2transport
encapsulation aal5
xconnect 10.13.13.13 100 encapsulation mpls
oam-ac emulation-enable 30
oam-pvc manage
```

### OAM Cell Emulation for ATM AAL5 over MPLS in VC Class Configuration Mode

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
pvc 1/200 l2transport
class-vc oamclass
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures OAM cell emulation for ATM AAL5 over MPLS in VC class configuration mode. The VC class is then applied to an interface. One PVC is configured with OAM cell emulation at an AIS rate of 10. That PVC uses the AIS rate of 10 instead of 30.

```
enable
configure terminal
vc-class atm oamclass
encapsulation aal5
oam-ac emulation-enable 30
oam-pvc manage
interface atm1/0
class-int oamclass
```

```
pvc 1/200 l2transport
oam-ac emulation-enable 10
xconnect 10.13.13.13 100 encapsulation mpls
```

## ATM Cell Relay over MPLS: Examples

### ATM Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to an interface.

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0
class-int cellrelay
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm cellrelay
encapsulation aal0
interface atm1/0
pvc 1/200 l2transport
class-vc cellrelay
xconnect 10.13.13.13 100 encapsulation mpls
```

### ATM Cell Relay over MPLS in PVP Mode

The following example transports single ATM cells over a virtual path:

```
pseudowire-class vp-cell-relay
encapsulation mpls
interface atm 5/0
atm pvp 1 l2transport
xconnect 10.0.0.1 123 pw-class vp-cell-relay
```

### ATM Cell Relay over MPLS in Port Mode

The following example shows interface ATM 5/0 configured to transport ATM cell relay packets:

```
pseudowire-class atm-cell-relay
encapsulation mpls
interface atm 5/0
xconnect 10.0.0.1 123 pw-class atm-cell-relay
```

The following example shows interface ATM 9/0/0 configured to transport ATM cell relay packets on a Cisco 7600 series router, where you must specify the interface ATM slot, bay, and port:

```
pseudowire-class atm-cell-relay
encapsulation mpls
interface atm 9/0/0
xconnect 10.0.0.1 500 pw-class atm-cell-relay
```



## ATM Single Cell Relay over MPLS: Examples

### ATM Packed Cell Relay over MPLS in VC Mode

The following example shows that ATM PVC 1/100 is an AToM cell relay PVC. There are three timers set up, with values of 1000 milliseconds, 800 milliseconds, and 500 milliseconds, respectively. The **cell-packing** command specifies that five ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 1 is to be used.

```
interface atm 1/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
pvc 1/100 l2transport
encapsulation aal0
xconnect 10.0.0.1 123 encapsulation mpls
cell-packing 5 mcpt-timer 1
```

### ATM Packed Cell Relay over MPLS in VC Mode Using VC Class Configuration Mode

The following example configures ATM cell relay over MPLS with cell packing in VC class configuration mode. The VC class is then applied to an interface.

```
enable
configure terminal
vc-class atm cellpacking
encapsulation aal0
cell-packing 10 mcpt-timer 1
interface atm1/0
shutdown
atm mcpt-timers 100 200 250
no shutdown
class-int cellpacking
pvc 1/200 l2transport
xconnect 10.13.13.13 100 encapsulation mpls
```

The following example configures ATM cell relay over MPLS in VC class configuration mode. The VC class is then applied to a PVC.

```
enable
configure terminal
vc-class atm cellpacking
encapsulation aal0
cell-packing 10 mcpt-timer 1
interface atm1/0
shutdown
atm mcpt-timers 100 200 250
no shutdown
pvc 1/200 l2transport
class-vc cellpacking
xconnect 10.13.13.13 100 encapsulation mpls
```

### ATM Packed Cell Relay over MPLS in VP Mode

The following example shows packed cell relay enabled on an interface configured for PVP mode. The **cell-packing** command specifies that 10 ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 2 is to be used.

```
interface atm 1/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
atm pvp 100 l2transport
```

```
xconnect 10.0.0.1 234 encapsulation mpls
cell-packing 10 mcpt-timer 2
```

### ATM Packed Cell Relay over MPLS in Port Mode

The following example shows packed cell relay enabled on an interface set up for port mode. The **cell-packing** command specifies that 10 ATM cells are to be packed into an MPLS packet. The **cell-packing** command also specifies that timer 2 is to be used.

```
interface atm 5/0
shutdown
atm mcpt-timer 1000 800 500
no shutdown
cell-packing 10 mcpt-timer 2
xconnect 10.0.0.1 123 encapsulation mpls
```

## Ethernet over MPLS: Examples

### Ethernet over MPLS in Port Mode

The following example configures VC 123 in Ethernet port mode:

```
pseudowire-class ethernet-port
encapsulation mpls

int gigabitethernet1/0
xconnect 10.0.0.1 123 pw-class ethernet-port
```

### Ethernet over MPLS with VLAN ID Rewrite

The following example configures VLAN ID rewrite on peer PE routers with Cisco 12000 series router engine 2 3-port Gigabit Ethernet line cards.

| PE1                                                                                                                                                               | PE2                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface GigabitEthernet0/0.2 encapsulation dot1Q 2 no ip directed-broadcast no cdp enable xconnect 10.5.5.5 2 encapsulation mpls remote circuit id 3</pre> | <pre>interface GigabitEthernet3/0.2 encapsulation dot1Q 3 no ip directed-broadcast no cdp enable xconnect 10.3.3.3 2 encapsulation mpls remote circuit id 2</pre> |

## Tunnel Selection: Examples

The following example sets up two preferred paths for PE1. One preferred path specifies an MPLS traffic engineering tunnel. The other preferred path specifies an IP address of a loopback address on PE2. There is a static route configured on PE1 that uses a TE tunnel to reach the IP address on PE2.

### PE1 Configuration

```
mpls label protocol ldp
mpls traffic-eng tunnels
tag-switching tdp router-id Loopback0
pseudowire-class pw1
  encapsulation mpls
  preferred-path interface Tunnell disable-fallback
!
pseudowire-class pw2
```

```
encapsulation mpls
preferred-path peer 10.18.18.18
!
interface Loopback0
 ip address 10.2.2.2 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 explicit name path-tul
!
interface Tunnel2
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 10.16.16.16
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1500
 tunnel mpls traffic-eng path-option 1 dynamic
!
interface gigabitethernet0/0/0
 no ip address
 no ip directed-broadcast
 no negotiation auto
!
interface gigabitethernet0/0/0.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 xconnect 10.16.16.16 101 pw-class pw1
!
interface ATM1/0/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
 encapsulation aal5
 xconnect 10.16.16.16 150 pw-class pw2
!
interface Ethernet2/0/1
 ip address 10.0.0.1 255.255.255.0
 no ip directed-broadcast
 tag-switching ip
 mpls traffic-eng tunnels
 ip rsvp bandwidth 15000 15000
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.2.2.2 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
ip route 10.18.18.18 255.255.255.255 Tunnel2
!
ip explicit-path name path-tul enable
 next-address 10.0.0.1
 index 3 next-address 10.0.0.1
```

**PE2 Configuration**

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback0
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Loopback2
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/1
 ip address 10.0.0.2 255.255.255.0
 no ip directed-broadcast
 mpls traffic-eng tunnels
 mpls ip
 no cdp enable
 ip rsvp bandwidth 15000 15000
!
interface Ethernet3/3
 no ip address
 no ip directed-broadcast
 no cdp enable
!
interface Ethernet3/3.1
 encapsulation dot1Q 222
 no ip directed-broadcast
 no cdp enable
 mpls l2transport route 10.2.2.2 101
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
 pvc 0/50 l2transport
  encapsulation aal5
  xconnect 10.2.2.2 150 encapsulation mpls
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.0.0.255 area 0
 network 10.16.16.16 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0

```

## Setting Frame Relay Discard Eligibility Bit on the Cisco 7200 and 7500 Series Routers: Examples

The following example shows how to configure the service policy called set-de and attach it to an interface. In this example, the class map called data evaluates all packets exiting the interface for an IP precedence value of 1. If the exiting packet has been marked with the IP precedence value of 1, the packet's DE bit is set to 1.

```

class-map data
 match ip precedence 1

policy-map set-de

```

```
class data
set fr-de
interface Serial0/0/0
encapsulation frame-relay
interface Serial0/0/0.1 point-to-point
ip address 192.168.249.194 255.255.255.252
frame-relay interface-dlci 100
service output set-de
```

## Matching Frame Relay DE Bit on the Cisco 7200 and 7500 Series Routers: Examples

The following example shows how to configure the service policy called match-de and attach it to an interface. In this example, the class map called data evaluates all packets entering the interface for a DE bit setting of 1. If the entering packet has been a DE bit value of 1, the packet's EXP bit setting is set to 3.

```
class-map data
match fr-de
policy-map match-de
class data
set mpls exp 3
ip routing
ip cef distributed
mpls label protocol ldp
interface Loopback0
 ip address 10.20.20.20 255.255.255.255
interface Ethernet1/0/0
 ip address 10.0.0.2 255.255.255.0
mpls ip
interface Serial4/0/0
 encapsulation frame-relay
service input match-de
connect 100 Serial4/0/0 100 l2transport
xconnect 10.10.10.10 100 encapsulation mpls
```

## ATM over MPLS: Examples

[Example 1](#) shows the configuration of ATM over MPLS on two PE routers.

**Example 1     ATM over MPLS Configuration Example**

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                   | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0  ip address 10.16.12.12 255.255.255.255 ! interface ATM4/0  pvc 0/100 l2transport   encapsulation aal0   xconnect 10.13.13.13 100 encapsulation mpls ! interface ATM4/0.300 point-to-point  no ip directed-broadcast  no atm enable-ilmi-trap  pvc 0/300 l2transport   encapsulation aal0   xconnect 10.13.13.13 300 encapsulation mpls </pre> | <pre> mpls label protocol ldp mpls ldp router-id Loopback0 force ! interface Loopback0  ip address 10.13.13.13 255.255.255.255 ! interface ATM4/0  pvc 0/100 l2transport   encapsulation aal0   xconnect 10.16.12.12 100 encapsulation mpls ! interface ATM4/0.300 point-to-point  no ip directed-broadcast  no atm enable-ilmi-trap  pvc 0/300 l2transport   encapsulation aal0   xconnect 10.16.12.12 300 encapsulation mpls </pre> |

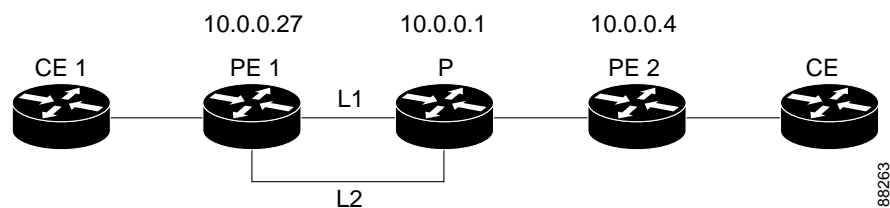
**Ethernet over MPLS with MPLS Traffic Engineering Fast Reroute: Examples**

The following configuration example and [Figure 2](#) show the configuration of Ethernet over MPLS with fast reroute on AToM PE routers.

Routers PE1 and PE2 have the following characteristics:

- A TE tunnel called Tunnel41 is configured between PE1 and PE2, using an explicit path through a link called L1. AToM VCs are configured to travel through the FRR-protected tunnel Tunnel41.
- The link L1 is protected by FRR, the backup tunnel is Tunnel1.
- PE2 is configured to forward the AToM traffic back to PE1 through the L2 link.

**Figure 2     Fast Reroute Configuration**

**PE1 Configuration**

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
pseudowire-class T41
 encapsulation mpls
 preferred-path interface Tunnel41 disable-fallback
!
pseudowire-class IP1
 encapsulation mpls
 preferred-path peer 10.4.0.1 disable-fallback
!
interface Loopback1

```

```

ip address 10.0.0.27 255.255.255.255
!
interface Tunnel1
ip unnumbered Loopback1
tunnel destination 10.0.0.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 10000
tunnel mpls traffic-eng path-option 1 explicit name FRR
!
interface Tunnel41
ip unnumbered Loopback1
tunnel destination 10.0.0.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name name-1
tunnel mpls traffic-eng fast-reroute
!
interface POS0/0
description pelname POS8/0/0
ip address 10.1.0.2 255.255.255.252
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel1
crc 16
clock source internal
pos ais-shut
pos report lrldi
ip rsvp bandwidth 155000 155000
!
interface POS0/3
description pelname POS10/1/0
ip address 10.1.0.14 255.255.255.252
mpls traffic-eng tunnels
crc 16
clock source internal
ip rsvp bandwidth 155000 155000
!
interface gigabitethernet3/0.1
encapsulation dot1Q 203
xconnect 10.0.0.4 2 pw-class IP1
!
interface gigabitethernet3/0.2
encapsulation dot1Q 204
xconnect 10.0.0.4 4 pw-class T41
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0
!
ip classless
ip route 10.4.0.1 255.255.255.255 Tunnel41
!
ip explicit-path name xxxx-1 enable
next-address 10.4.1.2
next-address 10.1.0.10

```

### P Configuration

```

ip cef
mpls traffic-eng tunnels
!
interface Loopback1

```

```

ip address 10.0.0.1 255.255.255.255
!
interface FastEthernet1/0/0
ip address 10.4.1.2 255.255.255.0
mpls traffic-eng tunnels
ip rsvp bandwidth 10000 10000
!
interface POS8/0/0
description xxxx POS0/0
ip address 10.1.0.1 255.255.255.252
mpls traffic-eng tunnels
pos ais-shut
pos report lrdi
ip rsvp bandwidth 155000 155000
!
interface POS10/1/0
description xxxx POS0/3
ip address 10.1.0.13 255.255.255.252
mpls traffic-eng tunnels
ip rsvp bandwidth 155000 155000
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
mpls traffic-eng router-id Loopback1
mpls traffic-eng area 0

```

### PE2 Configuration

```

ip cef
mpls label protocol ldp
mpls traffic-eng tunnels
mpls ldp router-id Loopback1 force
!
interface Loopback1
ip address 10.0.0.4 255.255.255.255
!
interface loopback 2
ip address 10.4.0.1 255.255.255.255
!
interface Tunnel27
ip unnumbered Loopback1
tunnel destination 10.0.0.27
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name xxxx-1
!
interface FastEthernet0/0.2
encapsulation dot1Q 203
xconnect 10.0.0.27 2 encapsulation mpls
!
interface FastEthernet0/0.3
encapsulation dot1Q 204
xconnect 10.0.0.27 4 encapsulation mpls
!
interface FastEthernet1/1
ip address 10.4.1.1 255.255.255.0
mpls traffic-eng tunnels
ip rsvp bandwidth 10000 10000
!
router ospf 1
network 10.0.0.0 0.255.255.255 area 0
mpls traffic-eng router-id Loopback1

```



```

mpls traffic-eng area 0
!
ip explicit-path name xxxx-1 enable
next-address 10.4.1.2
next-address 10.1.0.10

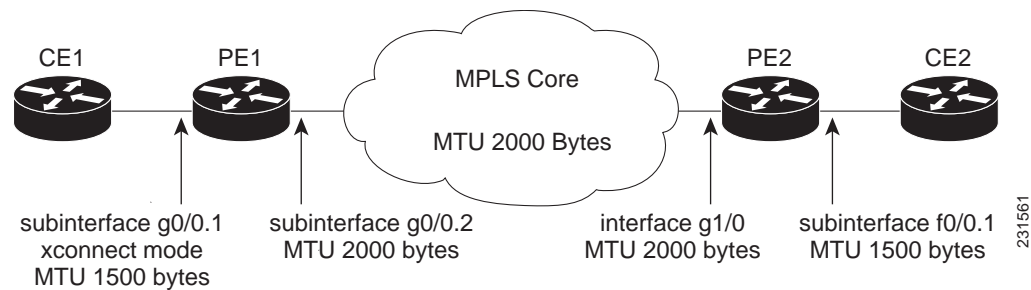
```

## Configuring per-Subinterface MTU for Ethernet over MPLS: Example

Figure 3 shows a configuration that enables matching MTU values between VC endpoints.

As shown in Figure 3, PE1 is configured in xconnect subinterface configuration mode with an MTU value of 1500 bytes in order to establish an end-to-end VC with PE2, which also has an MTU value of 1500 bytes. If PE1 was not set with an MTU value of 1500 bytes, in xconnect subinterface configuration mode, the subinterface would inherit the MTU value of 2000 bytes set on the interface. This would cause a mismatch in MTU values between the VC endpoints, and the VC would not come up.

**Figure 3** Configuring MTU Values in xconnect Subinterface Configuration Mode



The following examples show the router configurations in Figure 3:

### CE1 Configuration

```

interface gigabitethernet0/0
mtu 1500
no ip address
!
interface gigabitethernet0/0.1
encapsulation dot1Q 100
ip address 10.181.182.1 255.255.255.0

```

### PE1 Configuration

```

interface gigabitethernet0/0
mtu 2000
no ip address
!
interface gigabitethernet0/0.1
encapsulation dot1Q 100
xconnect 10.1.1.152 100 encapsulation mpls
mtu 1500
!
interface gigabitethernet0/0.2
encapsulation dot1Q 200
ip address 10.151.100.1 255.255.255.0
mpls ip

```

**PE2 Configuration**

```

interface gigabitethernet1/0
  mtu 2000
  no ip address
!
interface gigabitethernet1/0.2
  encapsulation dot1Q 200
  ip address 10.100.152.2 255.255.255.0
  mpls ip
!
interface fastethernet0/0
  no ip address
!
interface fastethernet0/0.1
  description default MTU of 1500 for FastEthernet
  encapsulation dot1Q 100
  xconnect 10.1.1.151 100 encapsulation mpls

```

**CE2 Configuration**

```

interface fastethernet0/0
  no ip address
interface fastethernet0/0.1
  encapsulation dot1Q 100
  ip address 10.181.182.2 255.255.255.0

```

The **show mpls l2transport binding** command, issued from router PE1, shows a matching MTU value of 1500 bytes on both the local and remote routers:

Router# **show mpls l2transport binding**

```

Destination Address: 10.1.1.152,  VC ID: 100
  Local Label: 100
    Cbit: 1,      VC Type: Ethernet,    GroupID: 0
    MTU: 1500,   Interface Desc: n/a
    VCCV: CC Type: CW [1], RA [2]
    CV Type: LSPV [2]
  Remote Label: 202
    Cbit: 1,      VC Type: Ethernet,    GroupID: 0
    MTU: 1500,   Interface Desc: n/a
    VCCV: CC Type: RA [2]
    CV Type: LSPV [2]

```

Router# **show mpls l2transport vc detail**

```

Local interface: Gi0/0.1 up, line protocol up, Eth VLAN 100 up
  Destination address: 10.1.1.152, VC ID: 100, VC status: up
    Output interface: Gi0/0.2, imposed label stack {202}
    Preferred path: not configured
    Default path: active
    Next hop: 10.151.152.2
  Create time: 1d11h, last status change time: 1d11h
  Signaling protocol: LDP, peer 10.1.1.152:0 up
    Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
    MPLS VC labels: local 100, remote 202
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description:
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 41, send 39
    byte totals:   receive 4460, send 5346
    packet drops:  receive 0, send 0

```

In the following example, you are specifying an MTU of 1501 in xconnect subinterface configuration mode, and that value is out of range, the router enters the command in subinterface configuration mode, where it is accepted:

```
Router# configure terminal
router(config)# interface gigabitethernet0/2.1
router(config-subif)# xconnect 10.10.10.1 100 encapsulation mpls
router(config-subif-xconn)# mtu ?
<64 - 1500> MTU size in bytes
router(config-subif-xconn)# mtu 1501
router(config-subif)# mtu ?
<64 - 17940> MTU size in bytes
```

If the MTU value is not accepted in either xconnect subinterface configuration mode or subinterface configuration mode, then the command is rejected, as shown in the following example:

```
Router# configure terminal
router(config)# interface gigabitethernet0/2.1
router(config-subif)# xconnect 10.10.10.1 100 encapsulation mpls
router(config-subif-xconn)# mtu ?
<64 - 1500> MTU size in bytes
router(config-subif-xconn)# mtu 63
% Invalid input detected at ^ marker
```

## Configuring MTU Values in xconnect Configuration Mode for L2VPN Interworking: Example

The following example shows an L2VPN Interworking example. The PE1 router has a serial interface configured with an MTU value of 1492 bytes. The PE2 router uses xconnect configuration mode to set a matching MTU of 1492 bytes, which allows the two routers to form an interworking VC. If the PE2 router did not set the MTU value in xconnect configuration mode, the interface would be set to 1500 bytes by default and the VC would not come up.

### PE1 Configuration

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.151 255.255.255.255
!
interface Serial2/0
 mtu 1492
 no ip address
 encapsulation ppp
 no fair-queue
 serial restart-delay 0
 xconnect 10.1.1.152 123 pw-class atom-ipiw
!
interface Serial4/0
 ip address 10.151.100.1 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.151 0.0.0.0 area 0
 network 10.151.100.0 0.0.0.3 area 0
```

```
!
mpls ldp router-id Loopback0
```

### PE2 Configuration

```
pseudowire-class atom-ipiw
 encapsulation mpls
 interworking ip
!
interface Loopback0
 ip address 10.1.1.152 255.255.255.255
!
interface Ethernet0/0
 no ip address
 xconnect 10.1.1.151 123 pw-class atom-ipiw
 mtu 1492
!
interface Serial4/0
 ip address 10.100.152.2 255.255.255.252
 encapsulation ppp
 mpls ip
 serial restart-delay 0
!
router ospf 1
 log-adjacency-changes
 network 10.1.1.152 0.0.0.0 area 0
 network 10.100.152.0 0.0.0.3 area 0
!
mpls ldp router-id Loopback0
```

The **show mpls l2transport binding** command shows that the MTU value for the local and remote routers is 1492 bytes.

### PE1 Configuration

```
Router# show mpls l2transport binding
```

```
Destination Address: 10.1.1.152, VC ID: 123
  Local Label: 105
    Cbit: 1, VC Type: PPP, GroupID: 0
    MTU: 1492, Interface Desc: n/a
    VCCV: CC Type: CW [1], RA [2]
    CV Type: LSPV [2]
  Remote Label: 205
    Cbit: 1, VC Type: Ethernet, GroupID: 0
    MTU: 1492, Interface Desc: n/a
    VCCV: CC Type: RA [2]
    CV Type: LSPV [2]
```

```
Router# show mpls l2transport vc detail
```

```
Local interface: Se2/0 up, line protocol up, PPP up
MPLS VC type is PPP, interworking type is IP
Destination address: 10.1.1.152, VC ID: 123, VC status: up
  Output interface: Se4/0, imposed label stack {1003 205}
  Preferred path: not configured
  Default path: active
  Next hop: point2point
Create time: 00:25:29, last status change time: 00:24:54
Signaling protocol: LDP, peer 10.1.1.152:0 up
Targeted Hello: 10.1.1.151(LDP Id) -> 10.1.1.152
Status TLV support (local/remote) : enabled/supported
Label/status state machine : established, LruRru
Last local dataplane status rcvd: no fault
```

```

Last local SSS circuit status rcvd: no fault
Last local SSS circuit status sent: no fault
Last local LDP TLV status sent: no fault
Last remote LDP TLV status rcvd: no fault
MPLS VC labels: local 105, remote 205
Group ID: local n/a, remote 0
MTU: local 1492, remote 1492
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 30, send 29
byte totals: receive 2946, send 3364
packet drops: receive 0, send 0

```

## PE2 Configuration

Router# **show mpls l2transport binding**

```

Destination Address: 10.1.1.151, VC ID: 123
Local Label: 205
  Cbit: 1, VC Type: Ethernet, GroupID: 0
  MTU: 1492, Interface Desc: n/a
  VCCV: CC Type: RA [2]
  CV Type: LSPV [2]
Remote Label: 105
  Cbit: 1, VC Type: Ethernet, GroupID: 0
  MTU: 1492, Interface Desc: n/a
  VCCV: CC Type: CW [1], RA [2]
  CV Type: LSPV [2]

```

Router# **show mpls l2transport vc detail**

```

Local interface: Et0/0 up, line protocol up, Ethernet up
MPLS VC type is Ethernet, interworking type is IP
Destination address: 10.1.1.151, VC ID: 123, VC status: up
Output interface: Se4/0, imposed label stack {1002 105}
Preferred path: not configured
Default path: active
Next hop: point2point
Create time: 00:25:19, last status change time: 00:25:19
Signaling protocol: LDP, peer 10.1.1.151:0 up
Targeted Hello: 10.1.1.152(LDP Id) -> 10.1.1.151
Status TLV support (local/remote) : enabled/supported
Label/status state machine : established, LruRru
Last local dataplane status rcvd: no fault
Last local SSS circuit status rcvd: no fault
Last local SSS circuit status sent: no fault
Last local LDP TLV status sent: no fault
Last remote LDP TLV status rcvd: no fault
MPLS VC labels: local 205, remote 105
Group ID: local n/a, remote 0
MTU: local 1492, remote 1492
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 29, send 30
byte totals: receive 2900, send 3426
packet drops: receive 0, send 0

```

## Removing a Pseudowire: Examples

The following example removes all xconnects:

```
Router# clear xconnect all
```

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

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

```
Router# clear xconnect peer 10.1.1.2 all
```

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

```

02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:08: XC AUTH [Et1/0.1, 1001]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:08: XC AUTH [10.1.1.2, 1234001]: Event: free xconnect authorization request, state
changed from DONE to END
02:14:08: MPLS peer 10.1.1.2 vcid 1234001, VC UP, VC state UP
02:14:08: MPLS peer 10.1.1.2 vcid 1234000, VC UP, VC state UP

```

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

```
Router# clear xconnect peer 10.1.1.2 vcid 1234001
```

```

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

```

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

```
Router# clear xconnect interface eth1/0.1
```

```

02:14:48: Xconnect[ac:Et1/0.1(Eth VLAN)]: provisioning fwder with fwd_type=1, sss_role=2
02:14:48: Xconnect[mpls:10.1.1.2:1234000]: provisioning fwder with fwd_type=2, sss_role=1
02:14:48: MPLS peer 10.1.1.2 vcid 1234000, VC DOWN, VC state DOWN
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: start xconnect authorization, state changed
from IDLE to AUTHORIZING
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: found xconnect authorization, state changed
from AUTHORIZING to DONE
02:14:48: XC AUTH [10.1.1.2, 1234000]: Event: free xconnect authorization request, state
changed from DONE to END

```

## Additional References

The following sections provide references related to the Any Transport over MPLS feature.

## Related Documents

| Related Topic                                             | Document Title                                                                                             |
|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Cisco IOS commands                                        | <a href="#">Cisco IOS Master Commands List, All Releases</a>                                               |
| MPLS commands                                             | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                  |
| Any Transport over MPLS                                   | “Overview” section of <a href="#">Cisco Any Transport over MPLS</a>                                        |
| Any Transport over MPLS for the Cisco 10000 series router | <a href="#">Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide</a> |
| Layer 2 Tunnel Protocol Version 3 (L2TPv3)                | <a href="#">Layer 2 Tunnel Protocol Version 3 (L2TPv3)</a>                                                 |
| L2VPN interworking                                        | <a href="#">L2VPN Interworking</a>                                                                         |

## Standards

| Standard                                  | Title                                                                  |
|-------------------------------------------|------------------------------------------------------------------------|
| draft-martini-l2circuit-trans-mpls-08.txt | <i>Transport of Layer 2 Frames Over MPLS</i>                           |
| draft-martini-l2circuit-encap-mpls-04.txt | <i>Encapsulation Methods for Transport of Layer 2 Frames Over MPLS</i> |

## MIBs

| MIB                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | MIBs Link                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>ATM AAL5 over MPLS and ATM Cell Relay over MPLS:</p> <ul style="list-style-type: none"> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> <li>• ATM MIB (ATM-MIB.my)</li> <li>• CISCO AAL5 MIB (CISCO-AAL5-MIB.my)</li> <li>• Cisco Enterprise ATM Extension MIB (CISCO-ATM-EXT-MIB.my)</li> <li>• Supplemental ATM Management Objects (CISCO-IETF-ATM2-PVCTRAP-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> </ul> <p>Ethernet over MPLS:</p> <ul style="list-style-type: none"> <li>• CISCO-ETHERLIKE-CAPABILITIES.my</li> <li>• Ethernet MIB (ETHERLIKE-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> </ul> <p>Frame Relay over MPLS:</p> <ul style="list-style-type: none"> <li>• Cisco Frame Relay MIB (CISCO-FRAME-RELAY-MIB.my)</li> <li>• Interfaces MIB (IF-MIB.my)</li> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> </ul> <p>HDLC and PPP over MPLS:</p> <ul style="list-style-type: none"> <li>• MPLS LDP MIB (MPLS-LDP-MIB.my)</li> <li>• Interface MIB (IF-MIB.my)</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://tools.cisco.com/go/mibs">http://tools.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                            |
|----------|----------------------------------|
| RFC 3032 | <i>MPLS Label Stack Encoding</i> |
| RFC 3036 | <i>LDP Specification</i>         |



## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for Any Transport over MPLS

[Table 8](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

[Table 8](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 8**      **Feature Information for Any Transport over MPLS**

| Feature Name            | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Any Transport over MPLS | 12.0(10)ST  | In Cisco IOS Release 12.0(10)ST, Any Transport over MPLS: ATM AAL5 over MPLS was introduced on the Cisco 12000 series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                         | 12.1(8a)E   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.0(21)ST  | In Cisco IOS Release 12.1(8a)E, Ethernet over MPLS was introduced on the Cisco 7600 series Internet router.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                         | 12.0(22)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.0(23)S   | In Cisco IOS Release 12.0(21)ST, Any Transport over MPLS: Ethernet over MPLS was introduced on the Cisco 12000 series routers. ATM AAL5 over MPLS was updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                         | 12.2(14)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.2(15)T   | In Cisco IOS Release 12.0(21)ST, Any Transport over MPLS: Ethernet over MPLS was introduced on the Cisco 12000 series routers. ATM AAL5 over MPLS was updated.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                         | 12.0(25)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.0(26)S   | In Cisco IOS Release 12.0(22)S, Ethernet over MPLS was integrated into this release. Support for the Cisco 10720 Internet router was added. ATM AAL5 over MPLS was integrated into this release for the Cisco 12000 series routers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|                         | 12.0(27)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.2(25)S   | In Cisco IOS Release 12.0(23)S, the following new features were introduced and support was added for them on the Cisco 7200 and 7500 series routers:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                         | 12.0(29)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.0(30)S   | <ul style="list-style-type: none"> <li>• ATM Cell Relay over MPLS (single cell relay, VC mode)</li> <li>• Frame Relay over MPLS</li> <li>• HDLC over MPLS</li> <li>• PPP over MPLS</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                         | 12.0(31)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.0(32)S   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.2(28)SB  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.4(11)T   | Cisco IOS Release 12.0(23)S also added support on the Cisco 12000, 7200, and 7500 series routers for the following features:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                         | 12.2(33)SRB |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.2(33)SXH | <ul style="list-style-type: none"> <li>• ATM AAL5 over MPLS</li> <li>• Ethernet over MPLS (VLAN mode)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                         | 12.2(33)SRC |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|                         | 12.2(33)SRD | <p>The AToM features were integrated into Cisco IOS Release 12.2(14)S.</p> <p>The AToM features were integrated into Cisco IOS Release 12.2(15)T.</p> <p>In Cisco IOS Release 12.0(25)S, the following new features were introduced:</p> <ul style="list-style-type: none"> <li>• New commands for configuring AToM</li> <li>• Ethernet over MPLS: port mode</li> <li>• ATM Cell Relay over MPLS: packed cell relay</li> <li>• ATM Cell Relay over MPLS: VP mode</li> <li>• ATM Cell Relay over MPLS: port mode</li> <li>• Distributed Cisco Express Forwarding mode for Frame Relay, PPP, and HDLC over MPLS</li> <li>• Fast reroute with AToM</li> <li>• Tunnel selection</li> <li>• Traffic policing</li> <li>• QoS support</li> </ul> |
|                         | 12.2(1)SRE  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Table 8**      **Feature Information for Any Transport over MPLS (continued)**

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>In Cisco IOS Release 12.0(26)S, the following new features were introduced:</p> <ul style="list-style-type: none"> <li>• Support for connecting disparate attachment circuits. See <i>L2VPN Interworking</i> for more information.</li> <li>• QoS functionality with AToM for the Cisco 7200 series routers.</li> </ul> <p>Support for FECN and BECN marking with Frame Relay over MPLS. (See <a href="#">BECN and FECN Marking for Frame Relay over MPLS</a> for more information.)</p> <p>In Cisco IOS Release 12.0(27)S, the following new features were introduced:</p> <ul style="list-style-type: none"> <li>• ATM Cell Relay over MPLS: Packed Cell Relay for VC, PVP, and port mode for the Cisco 12000 series router.</li> <li>• Support for ATM over MPLS on the Cisco 12000 series 4-port OC-12X/STM-4 ATM ISE line card.</li> </ul> <p>This feature was integrated into Cisco IOS Release 12.2(25)S for the Cisco 7200 and 7500 series routers.</p> <p>In Cisco IOS Release 12.0(29)S, the “Any Transport over MPLS Sequencing Support” feature was added for the Cisco 7200 and 7500 series routers. See the <a href="#">Any Transport over MPLS (AToM) Sequencing Support</a> document for more information.</p> <p>In Cisco IOS Release 12.0(30)S, the following new features were introduced:</p> <ul style="list-style-type: none"> <li>• ATM VC Class Support—You can specify AAL5 and AAL0 encapsulations as part of a VC class. You can also enable cell packing and OAM emulation as part of a VC class. A VC class can be attached to an interface, subinterface, or VC. See the “<a href="#">How to Configure Any Transport over MPLS</a>” section on page 14 for links to the sections that explain the ATM VC Class Support feature.</li> <li>• VLAN ID Rewrite—This feature was enhanced to enable the IP Service Engine (ISE) 4-port Gigabit Ethernet line card to perform VLAN ID rewrite at both the imposition and disposition sides of the edge-facing router. See the “<a href="#">Configuring Ethernet over MPLS with VLAN ID Rewrite</a>” section on page 48 for more information.</li> </ul> <p>In Cisco IOS Release 12.0(31)S, the Cisco 12000 series router introduced the following enhancements:</p> <ul style="list-style-type: none"> <li>• AToM VC Independence—With this enhancement, fast reroute is accomplished in less than 50 milliseconds, regardless of the number of VCs configured. See the “<a href="#">MPLS Traffic Engineering Fast Reroute</a>” section on page 6 for more information.</li> <li>• Support for ISE line cards on the 2.5G ISE SPA Interface Processor (SIP).</li> </ul> <p>In Cisco IOS Release 12.0(32)S, the Cisco 12000 series router added engine 5 line card support for the following transport types:</p> <ul style="list-style-type: none"> <li>• Ethernet over MPLS</li> <li>• Frame Relay over MPLS</li> <li>• HDLC over MPLS</li> <li>• PPP over MPLS</li> </ul> |

**Table 8**      **Feature Information for Any Transport over MPLS (continued)**

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>This feature was integrated into Cisco IOS Release 12.2(28)SB on the Cisco 10000 series routers. Platform-specific configuration information is contained in the “Configuring Any Transport over MPLS” section of the <a href="#">Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide</a>.</p> <p>Any Transport over MPLS was integrated into Cisco IOS Release 12.4(11)T with support for the following features:</p> <ul style="list-style-type: none"> <li>Any Transport over MPLS: Ethernet over MPLS: Port Mode</li> <li>Any Transport over MPLS: Ethernet over MPLS: VLAN Mode</li> <li>Any Transport over MPLS: Ethernet over MPLS: VLAN ID Rewrite</li> <li>Any Transport over MPLS: Frame Relay over MPLS</li> <li>Any Transport over MPLS: AAL5 over MPLS</li> <li>Any Transport over MPLS: ATM OAM Emulation</li> </ul> <p>AToM Tunnel Selection was introduced into this release on the Cisco 7600 router.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB to support the following features on the Cisco 7600 router:</p> <ul style="list-style-type: none"> <li>Any Transport over MPLS: Frame Relay over MPLS</li> <li>Any Transport over MPLS: ATM Cell Relay over MPLS: Packed Cell Relay</li> <li>Any Transport over MPLS: Ethernet over MPLS</li> <li><a href="#">AToM Static Pseudowire Provisioning</a></li> </ul> <p>Platform-specific configuration information is contained in the following documents:</p> <ul style="list-style-type: none"> <li>The “Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching” module of the <a href="#">Cisco 7600 Series Cisco IOS Software Configuration Guide</a>, Release 12.2SR</li> <li>The “Configuring Multiprotocol Label Switching on the Optical Services Modules” module of the <a href="#">OSM Configuration Note</a>, Release 12.2SR</li> <li>The “Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules” module of the <a href="#">FlexWAN and Enhanced FlexWAN Modules Configuration Guide</a></li> <li>The “Configuring Any Transport over MPLS on a SIP” section of the <a href="#">Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</a></li> <li>The “Configuring AToM VP Cell Mode Relay Support” section of the <a href="#">Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</a></li> <li>The <a href="#">Cross-Platform Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers</a></li> </ul> |

Table 8 Feature Information for Any Transport over MPLS (continued)

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH and supports the following features:</p> <ul style="list-style-type: none"> <li>Any Transport over MPLS: Ethernet over MPLS: Port Mode</li> <li>Any Transport over MPLS: AAL5 over MPLS</li> <li>Any Transport over MPLS: ATM OAM Emulation</li> <li>Any Transport over MPLS: Single Cell Relay—VC Mode</li> <li>Any Transport over MPLS: ATM Cell Relay over MPLS—VP Mode</li> <li>Any Transport over MPLS: Packed Cell Relay—VC/VP Mode</li> <li>Any Transport over MPLS: Ethernet over MPLS</li> <li>ATM Port Mode Packed Cell Relay over AToM</li> <li>AToM Tunnel Selection</li> </ul> <p>The following features were integrated into Cisco IOS Release 12.2(33)SRC:</p> <ul style="list-style-type: none"> <li>AToM Tunnel Selection for the Cisco 7200 and Cisco 7300 routers</li> <li>Per-Subinterface MTU for Ethernet over MPLS (EoMPLS)</li> </ul> <p>In Cisco IOS Release 12.2(33)SRD, support for ATM Cell Relay over MPLS in port mode on Cisco 7600 series routers was added.</p> <p>In Cisco IOS Release 12.2(1)SRE, support for control word on dynamic pseudowires was added. The <b>clear xconnect</b> command was introduced.</p> <ul style="list-style-type: none"> <li>The following commands were introduced or modified by this feature: <b>cell-packing</b>, <b>control-word</b>, <b>encapsulation (Any Transport over MPLS)</b>, <b>oam-ac emulation-enable</b>.</li> </ul> |

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

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

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

© 2001–2009 Cisco Systems, Inc. All rights reserved.



# MPLS MTU Command Changes

---

**First Published: August 11, 2004**

**Last Updated: December 8, 2009**

This document explains the change in behavior of the **mpls mtu** command for the following Cisco IOS releases:

- 12.2(27)SBC and later
- 12.2(33)SRA and later
- 12.4(11)T and later
- 12.2(33)SXH and later

You cannot set the MPLS MTU value larger than the interface MTU value. This eliminates problems, such as dropped packets, data corruption, and high CPU rates from occurring when MPLS MTU value settings are larger than interface MTU values. Cisco IOS software allows the MPLS MTU value to be higher than the interface MTU value only for interfaces that have a default interface MTU value of 1580 or less.



## Note

In Cisco IOS Release 15.0(1)M1, you can configure the interface MTU on PA-1FE and PA-2FE port adapters (PAs). The range of values is 1500 -1530. Before this enhancement, the MTU of those interfaces was not configurable. When you attempted to configure the interface MTU, the following message was displayed:

```
% Interface {Interface Name} does not support user settable mtu.
```

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS MTU Command Changes”](#) section on page 8.

## Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

# Contents

- [Information About MPLS MTU Command Changes, page 2](#)
- [How to Configure MPLS MTU Values, page 3](#)
- [Configuration Examples for Setting the MPLS MTU Values, page 5](#)
- [Feature Information for MPLS MTU Command Changes, page 8](#)

## Information About MPLS MTU Command Changes

Before configuring the interface or MPLS MTU values, you should understand the following concepts:

- [MPLS MTU Values During Upgrade, page 2](#)
- [Guidelines for Setting MPLS MTU and Interface MTU Values, page 2](#)
- [MPLS MTU Values for Ethernet Interfaces, page 3](#)

## MPLS MTU Values During Upgrade

If you have configuration files with MPLS MTU values that are larger than the interface MTU values and you upgrade to Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH or later releases, the software does not change the MPLS MTU value. When you reboot the router, the software accepts the values that are set for the MPLS MTU and the interface MTU. The following error message is displayed during system initialization:

```
Setting the mpls mtu to xxxx on interface x/x, which is higher than the interface MTU
xxxx. This could lead to packet forwarding problems including packet drops.
```

You must set the MPLS MTU values equal to or lower than the interface MTU values.

**Caution**

If you do not set the MPLS MTU less than or equal to the interface MTU, data corruption, dropped packets, and high CPU conditions can occur.

## Guidelines for Setting MPLS MTU and Interface MTU Values

When configuring the network to use MPLS, set the core-facing interface MTU values greater than the edge-facing interface MTU values, using one of the following methods:

- Set the interface MTU values on the core-facing interfaces to a higher value than the interface MTU values on the customer-facing interfaces to accommodate any packet labels, such as MPLS labels, that an interface might encounter. Make sure that the interface MTUs on the remote end interfaces have the same interface MTU values. The interface MTU values on both ends of the link must match.
- Set the interface MTU values on the customer-facing interfaces to a lower value than the interface MTU on the core-facing interfaces to accommodate any packet labels, such as MPLS labels, than an interface might encounter. When you set the interface MTU on the edge interfaces, ensure that the interface MTUs on the remote end interfaces have the same values. The interface MTU values on both ends of the link must match.



Changing the interface MTU can also modify the IP MTU, Connectionless Network Service (CLNS) MTU, and other MTU values, because they depend on the value of the interface MTU. The Open Shortest Path First (OSPF) routing protocol requires that the IP MTU values match on both ends of the link. Similarly, the Intermediate System-to-Intermediate System (IS-IS) routing protocol requires that the CLNS MTU values match on both ends of the link. If the values on both ends of the link do not match, IS-IS or OSPF cannot complete its initialization.

If the configuration of the adjacent router does not include the **mpls mtu** and **mtu** commands, add these commands to the router.

**Note**

The MPLS MTU setting is displayed only in the show running-config output if the MPLS MTU value is different from the interface MTU value. If the values match, only the interface MTU value is displayed.

If you attempt to set the MPLS MTU value higher than the interface MTU value, the software displays the following error, which reminds you to set the interface MTU to a higher value before you set the MPLS MTU value:

```
% Please increase interface mtu to xxxx and then set mpls mtu
```

**Note**

In Cisco IOS Release 15.0(1)M1, you can configure the interface MTU on PA-1FE and PA-2FE port adapters. The range of values is 1500 -1530. Before this enhancement, the MTU of those interfaces was not configurable.

## MPLS MTU Values for Ethernet Interfaces

If you have an interface with a default interface MTU value of 1580 or less (such as an Ethernet interface), the **mpls mtu** command provides an **override** keyword, which allows you to set the MPLS MTU value higher than the interface MTU value. The **override** keyword is not available for interface types that do not have a default interface MTU value of 1580 or less. For configuration details, see the [“Setting the MPLS MTU Value on an Ethernet Interface” section on page 5](#).

Setting the MPLS MTU value higher than the Ethernet interface MTU value can lead to dropped packets, data corruption, or high CPU rates. When you set the MPLS MTU value higher than the Ethernet interface MTU value, the software displays the following message:

```
%MFI-30-MPLS_MTU_SET: Setting the mpls mtu to xxxx on Ethernet x/x, which is higher than
the interface MTU xxxx. This could lead to packet forwarding problems including packet
drops.
Most drivers will be able to support baby giants and will gracefully drop packets that are
too large. Certain drivers will have packet forwarding problems including data corruption.
Setting the mpls mtu higher than the interface mtu can lead to packet forwarding problems
and may be blocked in a future release.
```

**Note**

The **override** keyword is supported in Cisco IOS Release 12.2(27)SBC, 12.2(33)SRA, 12.4(11)T, 12.2(33)SXH, and later releases, but may not be supported in a future release.

## How to Configure MPLS MTU Values

The following sections explain how to configure MPLS MTU and interface MTU values:

- [Setting the Interface MTU and MPLS MTU Values, page 4](#)

- [Setting the MPLS MTU Value on an Ethernet Interface, page 5](#)

## Setting the Interface MTU and MPLS MTU Values

Use the following steps to set the interface MTU and the MPLS MTU.



### Note

In Cisco IOS Release 15.0(1)M1, you can configure the interface MTU on PA-1FE and PA-2FE port adapters. The range of values is 1500 -1530. Before this enhancement, the MTU of those interfaces was not configurable.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mtu** *bytes*
5. **mpls mtu** *bytes*

### DETAILED STEPS

|        | Command or Action                                                                                     | Purpose                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                        | Enters global configuration mode.                                                                                     |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface Serial 1/0 | Enters interface configuration mode to configure the interface.                                                       |
| Step 4 | <b>mtu</b> <i>bytes</i><br><br><b>Example:</b><br>Router(config-if) mtu 1520                          | Sets the interface MTU size.                                                                                          |
| Step 5 | <b>mpls mtu</b> <i>bytes</i><br><br><b>Example:</b><br>Router(config-if) mpls mtu 1520                | Sets the MPLS MTU to match the interface MTU.                                                                         |


## Setting the MPLS MTU Value on an Ethernet Interface

Use the following steps to set the MPLS MTU value on an Ethernet interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls mtu override** *bytes*

### DETAILED STEPS

|        | Command or Action                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/0  | Enters interface configuration mode to configure the Ethernet interface.                                                                                                                                                                                                                                                          |
| Step 4 | <b>mpls mtu override</b> <i>bytes</i><br><br><b>Example:</b><br>Router(config-if) mpls mtu override 1510 | Sets the MPLS MTU to a value higher than the interface MTU value.<br><br><div>  <b>Caution</b> Setting the MPLS MTU value higher than the Ethernet interface MTU value can lead to dropped packets, data corruption, or high CPU rates. </div> |

## Configuration Examples for Setting the MPLS MTU Values

This section includes the following examples:

- [Setting the Interface MTU and MPLS MTU: Example, page 6](#)
- [Setting the MPLS MTU Value on an Ethernet Interface: Example, page 7](#)

## Setting the Interface MTU and MPLS MTU: Example

The following example shows how to set the interface and MPLS MTU values. The serial interface in the following configuration examples is at the default interface MTU value. The MPLS MTU value is not set. The interface settings are as follows:

```
interface Serial 4/0
  ip unnumbered Loopback0
  mpls traffic-eng tunnels
  mpls ip
  serial restart-delay 0
  ip rsvp bandwidth 2000 2000
end
```

The following example attempts to set the MPLS MTU value to 1520. This returns an error, because the MPLS MTU value cannot be set to a greater value than the interface MTU.

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface serial 4/0
```

```
Router(config-if)# mpls mtu 1520
```

```
% Please increase interface mtu to 1520 and then set mpls mtu
```

The following example first sets the interface MTU to 1520 and then sets the MPLS MTU to 1520:

```
Router(config-if)# mtu 1520
Router(config-if)# mpls mtu 1520
```

The following example shows the new interface MTU value. The MPLS MTU value is not displayed, because it is equal to the interface value.

```
Router# show running-config interface serial 4/0
```

```
Building configuration...
interface Serial4/0
  mtu 1520
  ip unnumbered Loopback0
  mpls traffic-eng tunnels
  mpls ip
  serial restart-delay 0
  ip rsvp bandwidth 2000 2000
end
```

The following example sets the MPLS MTU value to 1510:

```
Router(config-if)# mpls mtu 1510
```

The following example shows the new interface MTU value. The MPLS MTU value is displayed, because it is different than the interface MTU value.

```
Router# show running-config interface serial 4/0
```

```
Building configuration...
interface Serial4/0
  mtu 1520
  ip unnumbered Loopback0
  mpls mtu 1510
  mpls traffic-eng tunnels
  mpls ip
  serial restart-delay 0
  ip rsvp bandwidth 2000 2000
```

end

## Setting the MPLS MTU Value on an Ethernet Interface: Example



### Caution

Setting the MPLS MTU value higher than the Ethernet interface MTU value can lead to dropped packets, data corruption, or high CPU rates.

The following example shows how to set the MPLS MTU values on an Ethernet interface. The Ethernet interface in the following configuration examples is at the default interface MTU value. The MPLS MTU value is not set. The interface settings are as follows:

```
interface Ethernet 2/0
 ip unnumbered Loopback0
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 ip rsvp bandwidth 2000 2000
end
```

The following example uses the **override** keyword to set the MPLS MTU to 1520, which is higher than the Ethernet interface's MTU value:

```
Router(config-if)# mpls mtu override 1520
```

```
%MFI-30-MPLS_MTU_SET: Setting the mpls mtu to 1520 on Ethernet2/0, which is higher than
the interface MTU 1500. This could lead to packet forwarding problems including packet
drops.
```

The following example shows the new MPLS MTU value:

```
Router# show running-config interface ethernet 2/0
```

```
Building configuration...
interface Ethernet 2/0
 mtu 1500
 ip unnumbered Loopback0
 mpls mtu 1520
 mpls traffic-eng tunnels
 mpls ip
 serial restart-delay 0
 ip rsvp bandwidth 2000 2000
end
```

# Feature Information for MPLS MTU Command Changes

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase,

**Table 1** Feature Information for MPLS MTU Command Changes

| Feature Name             | Releases                                                                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS MTU Command Changes | 12.2(27)SBC<br>12.2(28)SB<br>12.2(33)SRA<br>12.4(11)T<br>12.2(33)SXH<br>15.0(1)M1 | <p>This document explains the changes to the <b>mpls mtu</b> command. You cannot set the MPLS MTU value larger than the interface MTU value, except for Ethernet interfaces.</p> <p>In 12.2(28)SB, support was added for the Cisco 10000 router.</p> <p>In 12.2(33)SRA, support was added for the Cisco 7600 series router.</p> <p>This feature was integrated into Cisco IOS Release 12.4(11)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>In 15.0(1)M1, you can configure the interface MTU on PA-1FE and PA-2FE port adapters.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About MPLS MTU Command Changes, page 2</a></li> <li>• <a href="#">How to Configure MPLS MTU Values, page 3</a></li> <li>• <a href="#">Configuration Examples for Setting the MPLS MTU Values, page 5</a></li> </ul> |

Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus,

Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

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

---

---

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

© 2009 Cisco Systems, Inc. All rights reserved.







# AToM Static Pseudowire Provisioning

---

**First Published: February 19, 2007**

**Last Updated: November 20, 2009**

The AToM Static Pseudowire Provisioning feature allows provisioning an Any Transport over Multiprotocol Label Switching (MPLS) (AToM) static pseudowire without the use of a directed control connection. In environments that do not or cannot use directed control protocols, this feature provides a means for provisioning the pseudowire parameters statically at the Cisco IOS command-line interface (CLI).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for AToM Static Pseudowire Provisioning”](#) section on page 9.

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

## Contents

- [Restrictions for AToM Static Pseudowire Provisioning, page 2](#)
- [Information About AToM Static Pseudowire Provisioning, page 2](#)
- [How to Provision an AToM Static Pseudowire, page 3](#)
- [Configuration Examples for AToM Static Pseudowire Provisioning, page 6](#)
- [Additional References, page 7](#)
- [Feature Information for AToM Static Pseudowire Provisioning, page 9](#)



---

**Americas Headquarters:**

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.

## Restrictions for AToM Static Pseudowire Provisioning

The following parameters are exchanged using directed control protocol messages on pseudowires, but cannot be changed using the AToM Static Pseudowire Provisioning feature introduced in Cisco IOS Release 12.33(SRB). Instead, the software has preconfigured defaults.

- The Virtual Circuit Connectivity Verification (VCCV) options used for fault detection, isolation, and verification at both ends of the connection are set as follows:
  - Control channel type 1 sets the control word.
  - Control channel type 2 sets the MPLS router alert label.
  - Connectivity verification type 2 sets the label switched path (LSP) **ping** command.

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

Autosensing of the virtual circuit type for Ethernet over MPLS is not supported.

Additionally, the following functionality is not supported for static pseudowires:

- Sequence number resynchronization—configured by the sequencing function in the Cisco IOS **pseudowire-class** command—is not supported because the sequence number resynchronization is done when the Label Distribution Protocol (LDP) software sends an LDP Label Release or Withdraw message followed by a Label Request or Mapping message, and static pseudowires do not use LDP.
- Tunnel stitching is not supported because it requires an extension of the Cisco IOS **neighbor** command to start the mode that allows configuring static pseudowire parameters such as remote and local labels, which is not supported in Cisco IOS Release 12.33(SRB). Note that a tunnel switch point can be configured using a different static label command. The tunnel switch point will not process control words, but label swapping will occur.
- Pseudowire redundancy is not supported because it requires using a directed control protocol between the peer provider edge routers.

## Information About AToM Static Pseudowire Provisioning

To provision an AToM static pseudowire, you should understand the following concepts:

- [Pseudowire Provisioning, page 2](#)
- [Benefits of Statically Provisioned Pseudowires, page 3](#)

## Pseudowire Provisioning

In software prior to Cisco IOS Release 12.33(SRB), pseudowires were dynamically provisioned using LDP, or another directed control protocol such as Resource Reservation Protocol over traffic-engineered tunnels (RSVP-TE), to exchange the various parameters required for these connections. In environments that do not or cannot use directed control protocols, a means for provisioning the pseudowire parameters statically at the Cisco IOS CLI is provided by the AToM Static Pseudowire Provisioning feature.

The AToM Static Pseudowire Provisioning feature is platform-independent, but has been tested on only the Cisco 7600 series routers for Cisco IOS Release 12.33(SRB).

# Benefits of Statically Provisioned Pseudowires

Cisco IOS Release 12.33(SRB) allows provisioning an AToM label switching static pseudowire without the use of a directed control connection. This feature also includes static provisioning of the tunnel label and the pseudowire label.

# How to Provision an AToM Static Pseudowire

This section contains the following procedures:

- [Provisioning an AToM Static Pseudowire, page 3](#)
- [Verifying the AToM Static Pseudowire Configuration, page 5](#)

# Provisioning an AToM Static Pseudowire

In this configuration task, you use options in the **xconnect** Ethernet interface configuration command to specify a static connection, and **mpls** commands in xconnect mode to statically set the following pseudowire parameters:

- Set the local and remote pseudowire labels
- Enable or disable sending the MPLS control word

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *ethernet-type interface-number*
4. **xconnect** *peer-ip-address vcid encapsulation mpls manual pw-class class-name*
5. **mpls label** *local-pseudowire-label remote-pseudowire-label*
6. **[no] mpls control-word**
7. **exit**

## DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |

|        | Command or Action                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface</b> <i>ethernet-type interface-number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 1/0                                                                                              | Enters interface configuration mode for the specified interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <b>xconnect</b> <i>peer-ip-address vcid encapsulation</i><br><b>mpls manual pw-class class-name</b><br><br><b>Example:</b><br>Router(config-if)# xconnect 10.131.191.252 100 encapsulation mpls manual pw-class mpls | Configures a static AToM pseudowire and enters xconnect configuration mode where the local and remote pseudowire labels are set.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 5 | <b>mpls label</b> <i>local-pseudowire-label remote-pseudowire-label</i><br><br><b>Example:</b><br>Router(config-if-xconn)# mpls label 100 150                                                                        | Sets the local and remote pseudowire labels. <ul style="list-style-type: none"> <li>The label must be an unused static label within the static label range configured using the <b>mpls label range</b> command.</li> <li>The <b>mpls label</b> command checks the validity of the label entered and displays an error message if it is not valid. The label supplied for the <i>remote-pseudowire-label</i> argument must be the value of the peer PE's local pseudowire label.</li> </ul>                                                                             |
| Step 6 | <b>[no] mpls control-word</b><br><br><b>Example:</b><br>Router(config-if-xconn)# no mpls control-word                                                                                                                | Sets whether the MPLS control word is sent. <ul style="list-style-type: none"> <li>This command must be set for Frame Relay data-link connection identifier (DLCI) and ATM adaptation layer 5 (AAL5) attachment circuits. For other attachment circuits, the control word is included by default.</li> <li>If you enable inclusion of the control word, it must be enabled on both ends of the connection for the circuit to work properly.</li> <li>Inclusion of the control word can be explicitly disabled using the <b>no mpls control-word</b> command.</li> </ul> |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if-xconn)# exit                                                                                                                                                  | Exits the configuration mode. <ul style="list-style-type: none"> <li>Continue entering the <b>exit</b> command at the router prompt until you reach the desired configuration mode.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                          |

## Verifying the AToM Static Pseudowire Configuration

To verify the AToM static pseudowire configuration, use the **show running-config EXEC** command. To verify that the AToM static pseudowire was provisioned correctly, use the **show mpls l2transport vc detail** and **ping mpls pseudowire** EXEC commands as described in the following steps.

### SUMMARY STEPS

1. **show mpls l2transport vc detail**
2. **ping mpls pseudowire *ipv4-address* *vc-id* *vc-id***

### DETAILED STEPS

#### Step 1 **show mpls l2transport vc detail**

For nonstatic pseudowire configurations, this command lists the type of protocol used to send the MPLS labels (such as LDP). For static pseudowire configuration, the value of the signaling protocol field should be Manual. Following is sample output:

```
Router# show mpls l2transport vc detail

Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 10.0.1.1, VC ID: 200, VC status: up
    Output interface: Et3/0, imposed label stack {17}
    Preferred path: not configured
    Default path:
      Next hop: 10.0.0.2
  Create time: 00:27:27, last status change time: 00:27:24
  Signaling protocol: Manual
    MPLS VC labels: local 17, remote 17
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 193, send 193
    byte totals:   receive 19728, send 23554
    packet drops:  receive 0, send 0
```

#### Step 2 **ping mpls pseudowire *ipv4-address* *vc-id* *vc-id***

Because there is no directed control protocol exchange of parameters on a static pseudowire, both ends of the connection must be correctly configured. One way to detect mismatch of labels or control word options is to send an MPLS pseudowire LSP **ping** command as part of configuration task, and then reconfigure the connection if problems are detected. An exclamation point (!) is displayed when the **ping** command is successfully sent to its destination. An example of command use and output follows:

```
Router# ping mpls pseudowire 10.7.1.2 vc-id 1001

Sending 5, 100-byte MPLS Echos to 10.7.1.2,
  timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

---

## Configuration Examples for AToM Static Pseudowire Provisioning

This section contains the following example:

- [Provisioning an AToM Pseudowire: Example, page 6](#)

### Provisioning an AToM Pseudowire: Example

The following examples show the configuration commands for an AToM static pseudowire connection between two PEs, PE1 and PE2.

The **mpls label range static** command must be used to configure the static label range prior to provisioning the AToM static pseudowire.

```
Router# configure terminal
Router(config)# mpls label range 200 16000 static 16 199
% Label range changes will take effect at the next reload.
```

The **mpls ip** command must also be configured on the core-facing interface of both PE1 and PE2 (which is also done for directed control protocol signaled pseudowires). Following is a configuration example:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# description Backbone interface
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# mpls ip
Router(config-if)# exit
```

Following is an example AToM static pseudowire configuration for PE1:

```
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.131.191.251 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 100 150
Router(config-if-xconn)# exit
```

Following is an example AToM static pseudowire configuration for PE2:

```
Router(config)# interface Ethernet 1/0
Router(config-if)# no ip address
Router(config-if)# xconnect 10.132.192.252 100 encapsulation mpls manual pw-class mpls
Router(config-if-xconn)# mpls label 150 100
Router(config-if-xconn)# exit
```

This feature also allows tunnel labels to be statically configured using the **mpls static binding ipv4 vrf** command. This means that there is no need to use a directed control protocol to provision tunnels and pseudowires. Refer to the [MPLS Static Labels](#) feature module and the [Cisco IOS Multiprotocol Label Switching Command Reference](#) for information about static labels and the **mpls static binding ipv4 vrf** command.

# Additional References

The following sections provide references related to the AToM Static Pseudowire Provisioning feature.

## Related Documents

| Related Topic                                                     | Document Title                                                                                                           |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS commands                                                | <a href="#">Cisco IOS Master Commands List, All Releases</a>                                                             |
| MPLS commands                                                     | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                |
| Configuring the pseudowire class                                  | <a href="#">Any Transport over MPLS</a>                                                                                  |
| MPLS and xconnect commands                                        | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                |
| Static labels and the <b>mpls static binding ipv4 vrf</b> command | “ <a href="#">MPLS Static Labels</a> ” section of the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> |

## Standards

| Standard                         | Title                                                                        |
|----------------------------------|------------------------------------------------------------------------------|
| IETF draft-ietf-pwe3-vccv-12.txt | <a href="#">Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)</a> |

## MIBs

| MIB  | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                             |
|----------|-----------------------------------|
| RFC 3036 | <a href="#">LDP Specification</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |



# Feature Information for AToM Static Pseudowire Provisioning

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for AToM Static Pseudowire Provisioning

| Feature Name                        | Releases                  | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AToM Static Pseudowire Provisioning | 12.2(33)SRB<br>12.2(1)SRE | <p>This feature allows provisioning an AToM static pseudowire without the use of a directed control protocol connection.</p> <p>The AToM Static Pseudowire feature is platform-independent, but has been tested on only the Cisco 7500 series routers for Cisco IOS Release 12.33(SRB).</p> <p>The following commands were introduced or modified by this feature: <b>cell-packing</b>, <b>mpls control-word</b>, <b>mpls label</b>, <b>show mpls l2transport vc</b>, <b>xconnect</b>.</p> |

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

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

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.





# MPLS Pseudowire Status Signaling

---

**First Published: December 31, 2007**

**Last Updated: February 27, 2009**

The MPLS Pseudowire Status Signaling feature enables you to configure the router so it can send pseudowire status to a peer router, even when the attachment circuit is down. In releases prior to Cisco IOS 12.2(33)SRC, if the attachment circuit was down, the pseudowire status messages were not sent to the peer.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Pseudowire Status Signaling”](#) section on page 9.

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

## Contents

- [Prerequisites for MPLS Pseudowire Status Signaling, page 2](#)
- [Restrictions for MPLS Pseudowire Status Signaling, page 2](#)
- [Information About MPLS Pseudowire Status Signaling, page 2](#)
- [How to Configure MPLS Pseudowire Status Signaling, page 4](#)
- [Configuration Examples for MPLS Pseudowire Status Signaling, page 5](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for MPLS Pseudowire Status Signaling, page 9](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS Pseudowire Status Signaling

- Before configuring this feature, make sure that both peer routers are capable of sending and receiving pseudowire status messages. Specifically, both routers should be running Cisco IOS Release 12.2(33)SRC and have the supported hardware installed.

## Restrictions for MPLS Pseudowire Status Signaling

- Both peer routers must support the ability to send and receive pseudowire status messages in label advertisement and label notification messages. If both peer routers do not support pseudowire status messages, Cisco recommends that you disable the messages with the **no status** command.
- This feature is not integrated with Any Transport over MPLS (AToM) Virtual Circuit Connection Verification (VCCV).
- This feature is not integrated with Bidirectional Forwarding Detection (BFD).
- The standby and required switchover values from IETF draft-muley-pwe3-redundancy-02.txt are not supported.
- For a list of supported hardware for this feature, see the release notes for your platform.

## Information About MPLS Pseudowire Status Signaling

Before configuring MPLS Pseudowire Status Signaling, you should understand the following concepts:

- [How MPLS Pseudowire Status Signaling Works](#)

## How MPLS Pseudowire Status Signaling Works

In releases prior to Cisco IOS Release 12.2(33)SRC, the control plane for AToM does not have the ability to provide pseudowire status. Therefore, when an attachment circuit (AC) associated with a pseudowire is down (or is forced down as part of the Pseudowire Redundancy functionality), labels advertised to peers are withdrawn. In Cisco IOS Release 12.2(33)SRC, the MPLS Pseudowire Status Signaling feature enables the AC status to be sent to the peer through the Label Distribution Protocol.

The pseudowire status messages are sent in label advertisement and label notification messages if the peer also supports the MPLS Pseudowire Status Signaling feature. You can issue the **show mpls l2transport vc detail** command to show that both the local and remote routers support pseudowire status messages. The following example shows the line of output to look for:

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```

## When One Router Does Not Support MPLS Pseudowire Status Signaling

The peer routers must support the ability to send and receive pseudowire status messages in label advertisement and label notification messages. If one router does not support pseudowire status messages, Cisco recommends that you disable the messages with the **no status** command. This returns the router to label withdraw mode.

If the peer does not support the MPLS Pseudowire Status Signaling feature, the local router changes its mode of operation to label withdraw mode. You can issue the **show mpls l2transport vc detail** command to show that the remote router does not support pseudowire status messages. The following example shows the line of output to look for:

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/not supported
```

When you issue the following **debug mpls l2transport vc** commands, the messages show that the peer router does not support the MPLS Pseudowire Status Signaling feature and that the local router is changing to withdraw mode, as shown in bold in the following example:

```
Router# debug mpls l2transport vc event
Router# debug mpls l2transport vc status event
Router# debug mpls l2transport vc status fsm
Router# debug mpls l2transport vc ldp

*Feb 26 13:41:40.707: ATOM LDP [110.1.1.2]: Sending label withdraw msg
*Feb 26 13:41:40.707: ATOM LDP [110.1.1.2]: VC Type 5, mtu 1500
*Feb 26 13:41:40.707: ATOM LDP [110.1.1.2]: VC ID 100, label 18
*Feb 26 13:41:40.707: ATOM LDP [110.1.1.2]: Status 0x0000000A [PW Status NOT supported]
```

## Status Messages Indicating That the Attachment Circuit Is Down

When the attachment circuit is down between the two routers, the output of the **show mpls l2transport vc detail** command shows the following status:

```
Router# show mpls l2transport vc detail
.
.
.
Last remote LDP TLV      status rcvd: AC DOWN(rx,tx faults)
```

The debug messages also indicate that the attachment circuit is down, as shown in bold in the command output:

```
Router# debug mpls l2transport vc event
Router# debug mpls l2transport vc status event
Router# debug mpls l2transport vc status fsm
Router# debug mpls l2transport vc ldp

*Feb 26 11:51:42.427: ATOM LDP [10.1.1.1]: Received notif msg, id 88
*Feb 26 11:51:42.427: ATOM LDP [10.1.1.1]: Status 0x00000007 [PW Status]
*Feb 26 11:51:42.427: ATOM LDP [10.1.1.1]: PW Status 0x00000006 [AC DOWN(rx,tx faults)]
```

Other pseudowire status messages include not-forwarding, pw-tx-fault, and pw-rx-fault.

## Message Codes in the Pseudowire Status Messages

The **debug mpls l2transport vc** and the **show mpls l2transport vc detail** commands show output that contains message codes. For example:

```
Label/status state machine: established, LruRru
```

```
AToM MGR [10.9.9.9, 100]: S:Evt local up, LndRru->LnuRru
```

The message codes (LruRru, LndRru, and LnuRru) indicate the status of the local and remote routers. You can use the following key to interpret the message codes:

L—local router

R—remote router

r or n—ready (r) or not ready (n)

u or d—up (u) or down (d) status

The output also includes other values:

D—Dataplane

S—Local shutdown

## How to Configure MPLS Pseudowire Status Signaling

This section explains how to perform the following tasks:

- [Enabling MPLS Pseudowire Status Signaling, page 4](#) (required)

### Enabling MPLS Pseudowire Status Signaling

Perform the following task to enable the router to send pseudowire status to a peer router even when the attachment circuit is down. If both routers do not support pseudowire status messages, then disable the messages with the **no status** command.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class *name***
4. **status**
5. **encapsulation mpls**
6. **exit**
7. **exit**
8. **show mpls l2transport vc detail**

## DETAILED STEPS

|        | Command or Action                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>pseudowire-class name</b><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom             | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.                                                                                                                                                                                                                                                                                                                        |
| Step 4 | <b>status</b><br><br><b>Example:</b><br>Router(config-pw)# status                                        | (Optional) Enables the router to send pseudowire status messages to the peer router through label advertisement and label notification messages.<br><br><b>Note</b> By default, status messages are enabled. This step is included only in case status messages have been disabled.<br><br>If you need to disable status messages because both peer routers do not support this functionality, enter the <b>no status</b> command. |
| Step 5 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw)# encapsulation mpls                | Specifies the tunneling encapsulation.                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pw)# exit                                            | Exits pseudowire class configuration mode.                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                               | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <b>show mpls l2transport vc detail</b><br><br><b>Example:</b><br>Router# show mpls l2transport vc detail | Validates that pseudowire messages can be sent and received.                                                                                                                                                                                                                                                                                                                                                                       |

## Configuration Examples for MPLS Pseudowire Status Signaling

This section contains the following examples:

[MPLS Pseudowire Status Signaling: Example](#)

[MPLS Pseudowire Status Signaling: Example](#)

## MPLS Pseudowire Status Signaling: Example

The following example configures the MPLS Pseudowire Status Signaling feature on two PE routers. By default, status messages are enabled. The **status** command is included in this example in case status messages have been disabled.

### PE1

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.255
!
pseudowire-class atomstatus
 encapsulation mpls
 status
!
interface GigabitEthernet10/5
 xconnect 10.1.1.2 123 pw-class atomstatus
```

### PE2

```
interface Loopback0
 ip address 10.1.1.2 255.255.255.255
!
pseudowire-class atomstatus
 encapsulation mpls
 status
!
interface GigabitEthernet3/3
 xconnect 10.1.1.1 123 pw-class atomstatus
```

## Verifying That Both Routers Support Pseudowire Status Messages: Example

You can issue the **show mpls l2transport vc detail** command to show that both the local and remote routers support pseudowire status messages. The following example shows the line of output to look for:

```
Router# show mpls l2transport vc detail
.
.
.
status TLV support (local/remote): enabled/supported
```



# Additional References

The following sections provide references related to the MPLS Pseudowire Status Signaling feature.

## Related Documents

| Related Topic                | Document Title                                                                      |
|------------------------------|-------------------------------------------------------------------------------------|
| Any Transport over MPLS      | <i><a href="#">Any Transport over MPLS</a></i>                                      |
| Virtual Private LAN Services | <i><a href="#">Virtual Private LAN Services on the Optical Services Modules</a></i> |

## Standards

| Standard                                | Title                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------|
| draft-ietf-pwe3-control-protocol-15.txt | <i>Pseudowire Setup and Maintenance Using LDP</i>                     |
| draft-ietf-pwe3-iana-allocation-08.txt  | <i>IANA Allocations for Pseudo Wire Edge to Edge Emulation (PWE3)</i> |
| draft-martini-pwe3-pw-switching-03.txt  | <i>Pseudo Wire Switching</i>                                          |

## MIBs

| MIB                                                                                | MIBs Link                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- **debug mpls l2transport vc**
- **show mpls l2transport vc**
- **status (pseudowire class)**

# Feature Information for MPLS Pseudowire Status Signaling

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Pseudowire Status Signaling

| Feature Name | Releases | Feature Information       |
|--------------|----------|---------------------------|
|              |          | Cisco 7600 series router. |

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.





# L2VPN Interworking

---

**First Published: August 26, 2003**

**Last Updated: November 20, 2009**

Layer 2 Virtual Private Network (L2VPN) Interworking allows you to connect disparate attachment circuits. This feature module explains how to configure the following L2VPN Interworking features:

- Ethernet/VLAN to ATM AAL5 Interworking
- Ethernet/VLAN to Frame Relay Interworking
- Ethernet/VLAN to PPP Interworking
- Ethernet to VLAN Interworking
- Frame Relay to ATM AAL5 Interworking
- Frame Relay to PPP Interworking
- Ethernet/VLAN to ATM virtual channel identifier (VPI) and virtual channel identifier (VCI) Interworking
- L2VPN Interworking: VLAN Enable/Disable Option for AToM

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for L2VPN Interworking”](#) section on page 31.

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

## Contents

- [Prerequisites for L2VPN Interworking, page 2](#)



---

**Americas Headquarters:**

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

- [Restrictions for L2VPN Interworking, page 2](#)
- [Information About L2VPN Interworking, page 11](#)
- [How to Configure L2VPN Interworking, page 15](#)
- [Configuration Examples for L2VPN Interworking, page 21](#)
- [Additional References, page 28](#)
- [Feature Information for L2VPN Interworking, page 31](#)

## Prerequisites for L2VPN Interworking

Before you configure L2VPN Interworking on a router:

- You must enable Cisco Express Forwarding.
- On the Cisco 12000 series Internet router, before you configure Layer 2 Tunnel Protocol version 3 (L2TPv3) for L2VPN Interworking on an IP Services Engine (ISE/Engine 3) or Engine 5 interface, you must also enable the L2VPN feature bundle on the line card.

To enable the feature bundle, enter the **hw-module slot np mode feature** command in global configuration mode as follows:

```
Router# configure terminal
Router(config)# hw-module slot slot-number np mode feature
```

## Restrictions for L2VPN Interworking

The following sections list the L2VPN Interworking restrictions:

- [General Restrictions, page 2](#)
- [Cisco 7600 Series Routers Restrictions, page 3](#)
- [Cisco 12000 Series Router Restrictions, page 5](#)
- [ATM AAL5 Interworking Restrictions, page 7](#)
- [Ethernet/VLAN Interworking Restrictions, page 8](#)
- [L2VPN Interworking: VLAN Enable/Disable Option for AToM Restrictions, page 9](#)
- [Frame Relay Interworking Restrictions, page 10](#)
- [PPP Interworking Restrictions, page 11](#)

## General Restrictions

This section lists general restrictions that apply to L2VPN Interworking. Other restrictions that are platform-specific or device-specific are listed in the following sections.

- The interworking type on one provider edge (PE) router must match the interworking type on the peer PE router.
- The following quality of service (QoS) features are supported with L2VPN Interworking:
  - Static IP type of service (ToS) or Multiprotocol Label Switching (MPLS) experimental bit (EXP) setting in tunnel header

- IP ToS reflection in tunnel header (Layer 2 Tunnel Protocol Version 3 (L2TPv3) only)
- Frame Relay policing
- Frame Relay data-link connection identifier (DLCI)-based congestion management (Cisco 7500/Versatile Interface Processor (VIP))
- One-to-one mapping of VLAN priority bits to MPLS EXP bits
- Only ATM AAL5 VC mode is supported; ATM VP and port mode are not supported.

## Cisco 7600 Series Routers Restrictions

The following line cards are supported on the Cisco 7600 series router. [Table 1](#) shows the line cards that are supported on the WAN (ATM, Frame Relay, or PPP) side of the interworking link. [Table 2](#) shows the line cards that are supported on the Ethernet side of the interworking link. For more details on the Cisco 7600 routers supported shared port adapters and line cards, see the following documents:

- [Cisco 7600 Series Routers Documentation Roadmap](#)
- [Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers](#)

**Table 1** Cisco 7600 Series Routers: Supported Line Cards for the WAN Side

| Interworking Type                           | Core-Facing Line Cards | Customer-Edge Line Cards       |
|---------------------------------------------|------------------------|--------------------------------|
| Ethernet (bridged)<br>(ATM and Frame Relay) | Any                    | EflexWAN<br>SIP-200<br>SIP-400 |
| IP (routed)<br>(ATM, Frame Relay, and PPP)  | Any                    | EflexWAN<br>SIP-200            |

**Table 2** Cisco 7600 Series Routers: Supported Line Cards for the Ethernet Side

| Interworking Type  | Ethernet over MPLS Mode                | Core-Facing Line Cards                                     | Customer-Edge Line Cards                                                                                    |
|--------------------|----------------------------------------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Ethernet (bridged) | Policy feature card (PFC) based        | Any, except optical service module (OSM) and ES40          | Catalyst LAN<br>SIP-600                                                                                     |
| Ethernet (bridged) | Switched virtual interface (SVI) based | EflexWAN<br>ES20<br>ES+40<br>SIP-200<br>SIP-400<br>SIP-600 | Catalyst LAN<br>EflexWAN (with MPB)<br>ES20<br>ES+40<br>SIP-200 (with MPB)<br>SIP-400 (with MPB)<br>SIP-600 |
| Ethernet (bridged) | Scalable (with E-MPB)                  | Any, except OSM                                            | ES20<br>SIP-600 and SIP-400 with Gigabit Ethernet (GE) SPA                                                  |

**Table 2** *Cisco 7600 Series Routers: Supported Line Cards for the Ethernet Side (continued)*

| Interworking Type | Ethernet over MPLS Mode | Core-Facing Line Cards                                                                                                                                                                                                                 | Customer-Edge Line Cards                                                                                                                                                            |
|-------------------|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP (routed)       | PFC-based               | Catalyst LAN SIP-600<br><br><b>Note:</b> PFC-based mode is not supported with routed interworking in Cisco IOS Release 12.2(33)SRD. Use SVI, Scalable, or Ethernet virtual connection (EVC) based Ethernet over MPLS (EoMPLS) instead. | Catalyst LAN SIP-600<br><br><b>Note:</b> PFC-based mode is not supported with routed interworking in Cisco IOS Release 12.2(33)SRD. Use SVI, Scalable, or EVC-based EoMPLS instead. |
| IP (routed)       | SVI-based               | Any, except Catalyst LAN and OSM.                                                                                                                                                                                                      | Catalyst LAN EflexWAN (with MPB) ES20<br>SIP-200 (with MPB)<br>SIP-400 (with MPB)<br>SIP-600                                                                                        |

The following restrictions apply to the Cisco 7600 series routers and L2VPN Interworking:

- OAM Emulation is not supported with L2VPN Interworking on the SIP-200, SIP-400, and Flexwan2 line cards.
- Cisco 7600 series routers support the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature starting in Cisco IOS Release 12.2(33)SRE. This feature has the following restrictions:
  - PFC-based EoMPLS is not supported.
  - Scalable and SVI-based EoMPLS are supported with the SIP-400 line card.
- The Cisco 7600 series routers do not support L2VPN Interworking over L2TPv3.
- Cisco 7600 series routers support only the following interworking types:
  - Ethernet/VLAN to Frame Relay (IP and Ethernet modes)
  - Ethernet/VLAN to ATM AAL5SNAP (IP and Ethernet modes)
  - Ethernet/VLAN to PPP (IP only)
  - Ethernet to VLAN Interworking
- Cisco 7600 series routers do not support the following interworking types:
  - Ethernet/VLAN to ATM AAL5MUX
  - Frame Relay to PPP Interworking
  - Frame Relay to ATM AAL5 Interworking
- Both ends of the interworking link must be configured with the same encapsulation and interworking type:



- If you use Ethernet encapsulation, you must use the Ethernet (bridged) interworking type. If you are not using Ethernet encapsulation, you can use a bridging mechanism, such as routed bridge encapsulation (RBE).
- If you use an IP encapsulation (such as ATM or Frame Relay), you must use the IP (routed) interworking type. The PE routers negotiate the process for learning and resolving addresses.
- You must use the same MTU size on the attachment circuits at each end of the pseudowire.
- PFC-based EoMPLS is not supported on ES40 line cards. SVI and EVC/scalable EoMPLS are the alternative options.
- PFC-based EoMPLS is not supported for Routed/IP interworking in Cisco IOS Release 12.2(33)SRD and later releases. The alternative Routed/IP interworking options are SVI and EVC or scalable EoMPLS. However, PFC-based EoMPLS is supported for Ethernet/Bridged interworking and for like-to-like over AToM.

## Cisco 12000 Series Router Restrictions

For more information about hardware requirements on the Cisco 12000 series routers, see the [Cross-Platform Release Notes for Cisco IOS Release 12.0S](#).

For QoS support on the Cisco 12000 series routers, see [Any Transport over MPLS \(AToM\): Layer 2 QoS \(Quality of Service\) for the Cisco 12000 Series Router](#)

### Frame Relay to PPP and High-Level Data Link Control Interworking

The Cisco 12000 series Internet router does not support L2VPN Interworking with PPP and high-level data link control (HDLC) transport types in Cisco IOS releases earlier than Cisco IOS Release 12.0(32)S.

In Cisco IOS Release 12.0(32)S and later releases, the Cisco 12000 series Internet router supports L2VPN interworking for Frame Relay over MPLS and PPP and HDLC over MPLS only on the following shared port adapters (SPAs):

- ISE/Engine 3 SPAs:
  - SPA-2XCT3/DS0 (2-port channelized T3 to DS0)
  - SPA-4XCT3/DS0 (4-port channelized T3 to DS0)
- Engine 5 SPAs:
  - SPA-1XCHSTM1/OC-3 (1-port channelized STM-1c/OC-3c to DS0)
  - SPA-8XCHT1/E1 (8-port channelized T1/E1)
  - SPA-2XOC-48-POS/RPR (2-port OC-48/STM16 POS/RPR)
  - SPA-OC-192POS-LR (1-port OC-192/STM64 POS/RPR)
  - SPA-OC-192POS-XFP (1-port OC-192/STM64 POS/RPR)

### L2VPN Interworking over L2TPv3

On the Cisco 12000 series Internet router, Ethernet (bridged) interworking is not supported for L2TPv3. Only IP (routed) interworking is supported.

IP (routed) interworking is not supported in an L2TPv3 pseudowire that is configured for data sequencing (using the **sequencing** command).

In Cisco IOS Release 12.0(32)SY and later releases, the Cisco 12000 series Internet router supports L2VPN Interworking over L2TPv3 tunnels in IP mode on ISE and Engine 5 line cards as follows:

- On an ISE interface configured for L2TPv3 tunneling, the following Layer 2 encapsulations are supported:
  - ATM adaptation layer type-5 (AAL5)
  - Ethernet
  - 802.1q (VLAN)
  - Frame Relay DLCI
- On an Engine 5 interface configured for L2TPv3 tunneling, the following Layer 2 encapsulations are supported:
  - Ethernet
  - 802.1q (VLAN)
  - Frame Relay DLCI

For more information, refer to [Layer 2 Tunnel Protocol Version 3](#).

The only frame format supported for L2TPv3 interworking on Engine 5 Ethernet SPAs is Ethernet Version 2 (also known as Ethernet II) with the Ether type 0x0800 value set as Internet Protocol Payload and (optionally) 802.1q VLAN. Ethernet packets with other Ethernet frame formats are dropped.

#### Remote Ethernet Port Shutdown Support

The Cisco Remote Ethernet Port Shutdown feature (which minimizes potential data loss after a remote link failure) is supported only on the following Engine 5 Ethernet SPAs:

- SPA-8XFE (8-port Fast Ethernet)
- SPA-2X1GE (2-port Gigabit Ethernet)
- SPA-5X1GE (5-port Gigabit Ethernet)
- SPA-10X1GE (10-port Gigabit Ethernet)
- SPA-1X10GE (1-port 10-Gigabit Ethernet)

For more information about this feature, refer to [Any Transport over MPLS \(AToM\): Remote Ethernet Port Shutdown](#).

#### L2VPN Any-to-Any Interworking on Engine 5 Line Cards

[Table 3](#) shows the different combinations of transport types supported for L2VPN interworking on Engine 3 and Engine 5 SPA interfaces connected through an attachment circuit over MPLS or L2TPv3.

**Table 3 Engine 3 and Engine 5 Line Cards/SPAs Supported for L2VPN Interworking**

| Attachment Circuit 1 (AC1) | Attachment Circuit 2 (AC2) | Interworking Mode | AC1 Engine Type and Line Card/SPA | AC2 Engine Type and Line Card/SPA |
|----------------------------|----------------------------|-------------------|-----------------------------------|-----------------------------------|
| Frame Relay                | Frame Relay                | IP                | Engine 5<br>POS and channelized   | Engine 3<br>ATM line cards        |
| Frame Relay                | ATM                        | Ethernet          | Engine 5<br>POS and channelized   | Engine 3<br>ATM line cards        |
| Frame Relay                | ATM                        | IP                | Engine 5<br>POS and channelized   | Engine 3<br>ATM line cards        |
| Frame Relay                | Ethernet                   | Ethernet          | Engine 5<br>POS and channelized   | Engine 5<br>Gigabit Ethernet      |

**Table 3**      **Engine 3 and Engine 5 Line Cards/SPAs Supported for L2VPN Interworking**

| <b>Attachment Circuit 1 (AC1)</b> | <b>Attachment Circuit 2 (AC2)</b> | <b>Interworking Mode</b> | <b>AC1 Engine Type and Line Card/SPA</b> | <b>AC2 Engine Type and Line Card/SPA</b> |
|-----------------------------------|-----------------------------------|--------------------------|------------------------------------------|------------------------------------------|
| Frame Relay                       | Ethernet                          | IP                       | Engine 5<br>POS and channelized          | Engine 5<br>Gigabit Ethernet             |
| Frame Relay                       | VLAN                              | Ethernet                 | Engine 5<br>POS and channelized          | Engine 5<br>Gigabit Ethernet             |
| Frame Relay                       | VLAN                              | IP                       | Engine 5<br>POS and channelized          | Engine 5<br>Gigabit Ethernet             |
| Ethernet                          | Ethernet                          | Ethernet                 | Engine 5<br>Gigabit Ethernet             | Engine 5<br>Gigabit Ethernet             |
| Ethernet                          | Ethernet                          | IP                       | Engine 5<br>Gigabit Ethernet             | Engine 5<br>Gigabit Ethernet             |
| Ethernet                          | VLAN                              | Ethernet                 | Engine 5<br>Gigabit Ethernet             | Engine 5<br>Gigabit Ethernet             |
| Ethernet                          | VLAN                              | IP                       | Engine 5<br>Gigabit Ethernet             | Engine 5<br>Gigabit Ethernet             |
| ATM                               | Ethernet                          | Ethernet                 | Engine 3<br>ATM line cards               | Engine 5<br>Gigabit Ethernet             |
| ATM                               | Ethernet                          | IP                       | Engine 3<br>ATM line cards               | Engine 5<br>Gigabit Ethernet             |

On the Cisco 12000 series Engine 3 line card, Network Layer Protocol ID (NLPID) encapsulation is not supported in routed mode; and neither NLPID nor AAL5MUX is supported in bridged mode.

- On the Cisco 12000 series Internet router, Ethernet (bridged) interworking is not supported for L2TPv3.

In an L2VPN Interworking configuration, after you configure L2TPv3 tunnel encapsulation for a pseudowire using the **encapsulation l2tpv3** command, you cannot enter the **interworking ethernet** command.

- On Ethernet SPAs on the Cisco 12000 series Internet router, the only frame format supported for L2TPv3 interworking is Ethernet Version 2 (also known as Ethernet II) with the Ether type 0x0800 value set as Internet Protocol Payload and [optionally] 802.1q VLAN.

Ethernet packets with other Ethernet frame formats are dropped.

## ATM AAL5 Interworking Restrictions

The following restrictions apply to ATM AAL5 Interworking:

- Switched virtual circuits (SVCs) are not supported.
- Inverse Address Resolution Protocol (ARP) is not supported with IP interworking.
- Customer edge (CE) routers must use point-to-point subinterfaces or static maps.
- Both AAL5MUX and AAL5SNAP encapsulation are supported. In the case of AAL5MUX, no translation is needed.
- In the Ethernet end-to-end over ATM scenario, the following translations are supported:

- Ethernet without LAN frame check sequence (FCS) (AAAA030080C200070000)
- Spanning tree (AAAA030080c2000E)

Everything else is dropped.

- In the IP over ATM scenario, the IPv4 (AAAA030000000800) translation is supported. Everything else is dropped.
- Operation, Administration, and Management (OAM) emulation for L2VPN Interworking is the same as like-to-like. The end-to-end F5 loopback cells are looped back on the PE router. When the pseudowire is down, an F5 end-to-end segment Alarm Indication Signal (AIS)/Remote Defect Identification (RDI) is sent from the PE router to the CE router.
- Interim Local Management Interface (ILMI) can manage virtual circuits (VCs) and permanent virtual circuits (PVCs).
- To enable ILMI management, configure ILMI PVC 0/16 on the PE router's ATM interface. If a PVC is provisioned or deleted, an ilmiVCCChange trap is sent to the CE router.
- Only the user side of the User-Network Interface (UNI) is supported; the network side of the UNI is not supported.

## Ethernet/VLAN Interworking Restrictions

The following restrictions apply to Ethernet/VLAN interworking:

- When you configure VLAN to Ethernet interworking, VLAN to Frame Relay (routed), or ATM using Ethernet (bridged) interworking, the PE router on the Ethernet side that receives a VLAN tagged frame from the CE router removes the VLAN tag. In the reverse direction, the PE router adds the VLAN tag to the frame before sending the frame to the CE router.  
(If you enable the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature with the **interworking vlan** command, VLAN ID is included as part of the Ethernet frame. See the [“VLAN Interworking” section on page 13](#) for more information. )
- In bridged interworking from VLAN to Frame Relay, the Frame Relay PE router does not strip off VLAN tags from the Ethernet traffic it receives.
- The Cisco 10720 Internet router supports Ethernet to VLAN Interworking Ethernet only over L2TPv3.
- Ethernet interworking for a raw Ethernet port or a VLAN trunk is not supported. Traffic streams are not kept separate when traffic is sent between transport types.
- In routed mode, only one CE router can be attached to an Ethernet PE router.
- There must be a one-to-one relationship between an attachment circuit and the pseudowire. Point-to-multipoint or multipoint-to-point configurations are not supported.
- Configure routing protocols for point-to-point operation on the CE routers when configuring an Ethernet to non-Ethernet setup.
- In the IP interworking mode, the IPv4 (0800) translation is supported. The PE router captures ARP (0806) packets and responds with its own MAC address (proxy ARP). Everything else is dropped.
- The Ethernet or VLAN must contain only two IP devices: PE router and CE router. The PE router performs proxy ARP and responds to all ARP requests it receives. Therefore, only one CE and one PE router should be on the Ethernet or VLAN segment.
- If the CE routers are doing static routing, you can perform the following tasks:

- The PE router needs to learn the MAC address of the CE router to correctly forward traffic to it. The Ethernet PE router sends an Internet Control Message Protocol (ICMP) Router discovery protocol (RDP) solicitation message with the source IP address as zero. The Ethernet CE router responds to this solicitation message. To configure the Cisco CE router's Ethernet or VLAN interface to respond to the ICMP RDP solicitation message, issue the **ip irdp** command in interface configuration mode. If you do not configure the CE router, traffic is dropped until the CE router sends traffic toward the PE router.
- To disable the CE routers from running the router discovery protocol, issue the **ip irdp maxadvertinterval 0** command in interface mode.
- This restriction applies if you configure interworking between Ethernet and VLAN with Catalyst switches as the CE routers. The spanning tree protocol is supported for Ethernet interworking. Ethernet interworking between an Ethernet port and a VLAN supports spanning tree protocol only on VLAN 1. Configure VLAN 1 as a nonnative VLAN.
- When you change the interworking configuration on an Ethernet PE router, clear the ARP entry on the adjacent CE router so that it can learn the new MAC address. Otherwise, you might experience traffic drops.

## L2VPN Interworking: VLAN Enable/Disable Option for AToM Restrictions

The following restrictions apply to the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature, which allows the VLAN ID to be included as part of the Ethernet frame:

- The L2VPN Interworking: VLAN Enable/Disable Option for AToM feature is supported on the following releases:
  - Cisco IOS release 12.2(52)SE for the Cisco Catalyst 3750 Metro switches
  - Cisco IOS Release 12.2(33)SRE for the Cisco 7600 series routers
- L2VPN Interworking: VLAN Enable/Disable Option for AToM is not supported with L2TPv3. You can configure the feature only with AToM.
- If the interface on the PE router is a VLAN interface, it is not necessary to specify the **interworking vlan** command on that PE router.
- The L2VPN Interworking: VLAN Enable/Disable Option for AToM feature works only with the following attachment circuit combinations:
  - Ethernet to Ethernet
  - Ethernet to VLAN
  - VLAN to VLAN
- If you specify an interworking type on a PE router, that interworking type must be enforced. The interworking type must match on both PE routers. Otherwise, the VC may be in an incompatible state and remain in the down state. If the attachment circuit (AC) is VLAN, the PE router can negotiate (autosense) the VC type using Label Distribution Protocol (LDP).

For example, both PE1 and PE2 use Ethernet interfaces, and VLAN interworking is specified on PE1 only. PE2 is not configured with an interworking type and cannot autosense the interworking type. The result is an incompatible state where the VC remains in the down state.

On the other hand, if PE1 uses an Ethernet interface and VLAN interworking is enabled (which will enforce VLAN as the VC type), and PE2 uses a VLAN interface and interworking is not enabled (which causes PE2 to use Ethernet as its default VC type), PE2 can autosense and negotiate the interworking type and select VLAN as the VC type.

Table 4 summarizes shows the AC types, interworking options, and VC types after negotiation.

**Table 4** *Negotiating Ethernet and VLAN Interworking Types*

| PE1 AC Type | Interworking Option | PE2 AC Type | Interworking Option | VC Type after Negotiation |
|-------------|---------------------|-------------|---------------------|---------------------------|
| Ethernet    | none                | Ethernet    | none                | Ethernet                  |
| Vlan        | none                | Ethernet    | none                | Ethernet                  |
| Ethernet    | none                | Vlan        | none                | Ethernet                  |
| Vlan        | none                | Vlan        | none                | Ethernet                  |
| Ethernet    | Vlan                | Ethernet    | none                | Incompatible              |
| Vlan        | Vlan                | Ethernet    | none                | Incompatible              |
| Ethernet    | Vlan                | Vlan        | none                | Vlan                      |
| Vlan        | Vlan                | Vlan        | none                | Vlan                      |
| Ethernet    | none                | Ethernet    | Vlan                | Incompatible              |
| Vlan        | none                | Ethernet    | Vlan                | Vlan                      |
| Ethernet    | none                | Vlan        | Vlan                | Incompatible              |
| Vlan        | none                | Vlan        | Vlan                | Vlan                      |
| Ethernet    | Vlan                | Ethernet    | Vlan                | Vlan                      |
| Vlan        | Vlan                | Ethernet    | Vlan                | Vlan                      |
| Ethernet    | Vlan                | Vlan        | Vlan                | Vlan                      |
| Vlan        | Vlan                | Vlan        | Vlan                | Vlan                      |

## Frame Relay Interworking Restrictions

The following restrictions apply to Frame Relay interworking:

- The attachment circuit maximum transmission unit (MTU) sizes must match when you connect them over MPLS. By default, the MTU size associated with a Frame Relay DLCI is the interface MTU. This may cause problems, for example, when connecting some DLCIs on a PoS interface (with a default MTU of 4470 bytes) to Ethernet or VLAN (with a default MTU of 1500 bytes) and other DLCIs on the same PoS interface to ATM (with a default MTU of 4470 bytes). To avoid reducing all the interface MTUs to the lowest common denominator (1500 bytes in this case), you can specify the MTU for individual DLCIs using the **mtu** command.
- Only DLCI mode is supported. Port mode is not supported.
- Configure Frame Relay switching to use DCE or Network-to-Network Interface (NNI). DTE mode does not report status in the Local Management Interface (LMI) process. If a Frame Relay over MPLS circuit goes down and the PE router is in DTE mode, the CE router is never informed of the disabled circuit. You must configure the **frame-relay switching** command in global configuration mode in order to configure DCE or NNI.
- Frame Relay policing is non-distributed on the Cisco 7500 series routers. If you enable Frame Relay policing, traffic is sent to the route switch processor for processing.
- Inverse ARP is not supported with IP interworking. CE routers must use point-to-point subinterfaces or static maps.

- The PE router automatically supports translation of both the Cisco encapsulations and the Internet Engineering Task Force (IETF) encapsulations that come from the CE, but translates only to IETF when sending to the CE router. This is not a problem for the Cisco CE router, because it can handle IETF encapsulation on receipt even if it is configured to send Cisco encapsulation.
- With Ethernet interworking, the following translations are supported:
  - Ethernet without LAN FCS (0300800080C20007 or 6558)
  - Spanning tree (0300800080C2000E or 4242)

All other translations are dropped.

- With IP interworking, the IPv4 (03CC or 0800) translation is supported. All other translations are dropped.
- PVC status signaling works the same way as in like-to-like case. The PE router reports the PVC status to the CE router, based on the availability of the pseudowire. PVC status detected by the PE router will also be reflected into the pseudowire. LMI to OAM interworking is supported when you connect Frame Relay to ATM.

## PPP Interworking Restrictions

The following restrictions apply to PPP interworking:

- There must be a one-to-one relationship between a PPP session and the pseudowire. Multiplexing of multiple PPP sessions over the pseudowire is not supported.
- There must be a one-to-one relationship between a PPP session and a Frame Relay DLCI. Each Frame Relay PVC must have only one PPP session.
- Only IP (IPv4 (0021) interworking is supported. Link Control Protocol (LCP) packets and Internet Protocol Control Protocol (IPCP) packets are terminated at the PE router. Everything else is dropped.
- Proxy IPCP is automatically enabled on the PE router when IP interworking is configured on the pseudowire.
- By default, the PE router assumes that the CE router knows the remote CE router's IP address.
- Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP) authentication are supported.

## Information About L2VPN Interworking

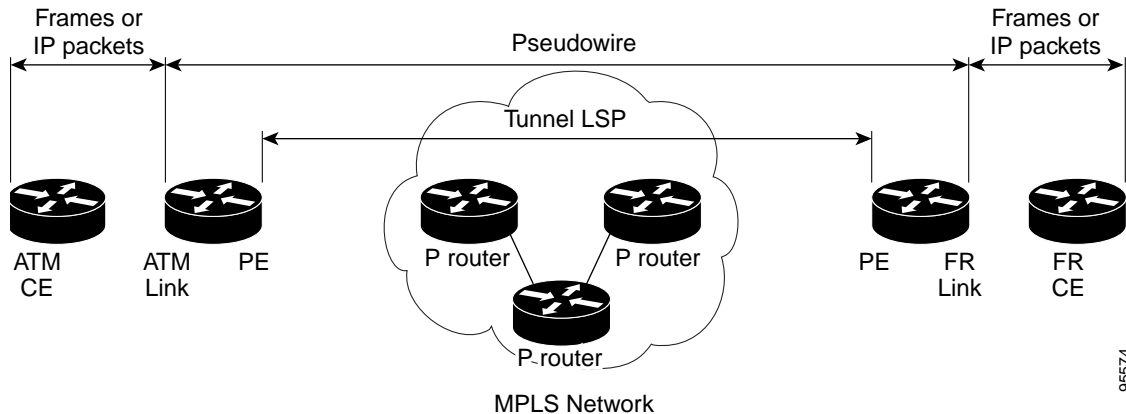
The following sections provide an introduction to L2VPN interworking.

- [Overview of L2VPN Interworking, page 12](#)
- [L2VPN Interworking Modes, page 12](#)
- [L2VPN Interworking: Support Matrix, page 14](#)
- [Static IP Addresses for L2VPN Interworking for PPP, page 14](#)

## Overview of L2VPN Interworking

Layer 2 transport over MPLS and IP already exists for like-to-like attachment circuits, such as Ethernet-to-Ethernet or PPP-to-PPP. L2VPN Interworking builds on this functionality by allowing disparate attachment circuits to be connected. An interworking function facilitates the translation between the different Layer 2 encapsulations. [Figure 1](#) is an example of Layer 2 interworking, where ATM and Frame Relay packets travel over the MPLS cloud.

**Figure 1** *ATM to Frame Relay Interworking Example*



The L2VPN Interworking feature supports Ethernet, 802.1Q (VLAN), Frame Relay, ATM AAL5, and PPP attachment circuits over MPLS and L2TPv3. The features and restrictions for like-to-like functionality also apply to L2VPN Interworking.

## L2VPN Interworking Modes

L2VPN Interworking works in either Ethernet (“bridged”) mode, IP (“routed”), or Ethernet VLAN mode. You specify the mode by issuing the **interworking {ethernet | ip | vlan}** command in pseudowire-class configuration mode.

### Ethernet (Bridged) Interworking

The **ethernet** keyword causes Ethernet frames to be extracted from the attachment circuit and sent over the pseudowire. Ethernet end-to-end transmission is assumed. Attachment circuit frames that are not Ethernet are dropped. In the case of VLAN, the VLAN tag is removed, leaving an untagged Ethernet frame.

Ethernet Interworking is also called bridged interworking. Ethernet frames are bridged across the pseudowire. The CE routers could be natively bridging Ethernet or could be routing using a bridged encapsulation model, such as Bridge Virtual Interface (BVI) or RBE. The PE routers operate in Ethernet like-to-like mode.

This mode is used to offer the following services:

95574



- LAN services—An example is an enterprise that has several sites, where some sites have Ethernet connectivity to the service provider (SP) network and others have ATM connectivity. The enterprise wants LAN connectivity to all its sites. In this case, traffic from the Ethernet or VLAN of one site can be sent through the IP/MPLS network and encapsulated as bridged traffic over an ATM VC of another site.
- Connectivity services—An example is an enterprise that has different sites that are running an Internal Gateway Protocol (IGP) routing protocol, which has incompatible procedures on broadcast and nonbroadcast links. The enterprise has several sites that are running an IGP, such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS), between the sites. In this scenario, some of the procedures (such as route advertisement or designated router) depend on the underlying Layer 2 protocol and are different for a point-to-point ATM connection versus a broadcast Ethernet connection. Therefore, the bridged encapsulation over ATM can be used to achieve homogenous Ethernet connectivity between the CE routers running the IGP.

## IP (Routed) Interworking

The **ip** keyword causes IP packets to be extracted from the attachment circuit and sent over the pseudowire. Attachment circuit frames that do not contain IPv4 packets are dropped.

IP Interworking is also called routed interworking. The CE routers encapsulate IP on the link between the CE and PE routers. A new VC type is used to signal the IP pseudowire in MPLS and L2TPv3. Translation between the Layer 2 and IP encapsulations across the pseudowire is required. Special consideration needs to be given to address resolution and routing protocol operation, because these are handled differently on different Layer 2 encapsulations.

This mode is used to provide IP connectivity between sites, regardless of the Layer 2 connectivity to these sites. It is different from a Layer 3 VPN because it is point-to-point in nature and the service provider does not maintain any customer routing information.

Address resolution is encapsulation dependent:

- Ethernet uses ARP
- Frame Relay and ATM use Inverse ARP
- PPP uses IPCP

Therefore, address resolution must be terminated on the PE router. End-to-end address resolution is not supported. Routing protocols operate differently over broadcast and point-to-point media. For Ethernet, the CE routers must either use static routing or configure the routing protocols to treat the Ethernet side as a point-to-point network.

## VLAN Interworking

The **vlan** keyword allows the VLAN ID to be included as part of the Ethernet frame. In Cisco IOS Release 12.2(52)SE, you can configure Catalyst 3750 Metro switches to use Ethernet VLAN for Ethernet (bridged) interworking. You can specify the Ethernet VLAN (type 4) by issuing the **interworking vlan** command in pseudowire-class configuration mode. This allows the VLAN ID to be included as part of the Ethernet frame. In releases previous to Cisco IOS Release 12.2(52)SE, the only way to achieve VLAN encapsulation is to ensure the CE router is connected to the PE router through an Ethernet VLAN interface/subinterface.

## L2VPN Interworking: Support Matrix

The supported L2VPN Interworking features are listed in [Table 5](#).

**Table 5** *L2VPN Interworking Supported Features*

| Feature                                                 | MPLS or L2TPv3 Support             | IP or Ethernet Support      |
|---------------------------------------------------------|------------------------------------|-----------------------------|
| Ethernet/VLAN to ATM AAL5                               | MPLS<br>L2TPv3 (12000 series only) | IP<br>Ethernet              |
| Ethernet/VLAN to Frame Relay                            | MPLS<br>L2TPv3                     | IP<br>Ethernet              |
| Ethernet/VLAN to PPP                                    | MPLS                               | IP                          |
| Ethernet to VLAN                                        | MPLS<br>L2TPv3                     | IP<br>Ethernet <sup>1</sup> |
| L2VPN Interworking: VLAN Enable/Disable Option for AToM | MPLS                               | Ethernet VLAN               |
| Frame Relay to ATM AAL5                                 | MPLS<br>L2TPv3 (12000 series only) | IP                          |
| Frame Relay to Ethernet or VLAN                         | MPLS<br>L2TPv3                     | IP<br>Ethernet              |
| Frame Relay to PPP                                      | MPLS<br>L2TPv3                     | IP                          |

**Note:** On the Cisco 12000 series Internet router:

- Ethernet (bridged) interworking is not supported for L2TPv3.
- IP (routed) interworking is not supported in an L2TPv3 pseudowire configured for data sequencing (using the **sequencing** command).

1. With the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature, VLAN interworking can also be supported. For more information, see the [“VLAN Interworking”](#) section on page 13.

## Static IP Addresses for L2VPN Interworking for PPP

If the PE router needs to perform address resolution with the local CE router for PPP, you can configure the remote CE router's IP address on the PE router. Issue the **ppp ipcp address proxy** command with the remote CE router's IP address on the PE router's xconnect PPP interface. The following example shows a sample configuration:

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

interface Serial2/0
 encapsulation ppp
 xconnect 10.0.0.2 200 pw-class ip-interworking
 ppp ipcp address proxy 10.65.32.14
```

You can also configure the remote CE router's IP address on the local CE router with the **peer default ip address** command if the local CE router performs address resolution.

# How to Configure L2VPN Interworking

The following sections explain the tasks you can perform to configure L2VPN Interworking:

- [Configuring L2VPN Interworking, page 15](#) (required)
- [Verifying the L2VPN Interworking Configuration, page 16](#) (optional)
- [Configuring L2VPN Interworking: VLAN Enable/Disable Option for AToM, page 19](#) (optional)

## Configuring L2VPN Interworking

L2VPN Interworking allows you to connect disparate attachment circuits. Configuring the L2VPN Interworking feature requires that you add the **interworking** command to the list of commands that make up the pseudowire. The steps for configuring the pseudowire for L2VPN Interworking are included in this section. You use the **interworking** command as part of the overall AToM or L2TPv3 configuration. For specific instructions on configuring AToM or L2TPv3, see the following documents:

- [Layer 2 Tunnel Protocol Version 3](#)
- [Any Transport over MPLS](#)

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hw-module slot *slot-number* np mode feature**
4. **pseudowire-class *name***
5. **encapsulation {mpls | l2tpv3}**
6. **interworking {ethernet | ip | vlan}**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                            |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                    |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                    |

|               | Command or Action                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <pre>hw-module slot <i>slot-number</i> np mode feature</pre> <p><b>Example:</b><br/>Router(config)# hw-module slot 3 np mode feature</p> | <p>(Optional) Enables L2VPN Interworking functionality on the Cisco 12000 series router.</p> <p><b>Note</b> Enter this command only on a Cisco 12000 series Internet router if you use L2TPv3 for L2VPN Interworking on an ISE (Engine 3) or Engine 5 interface.<br/>In this case, you must first enable the L2VPN feature bundle on the line card by entering the <b>hw-module slot <i>slot-number</i> np mode feature</b> command.</p> |
| <b>Step 4</b> | <pre>pseudowire-class <i>name</i></pre> <p><b>Example:</b><br/>Router(config)# pseudowire-class class1</p>                               | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.                                                                                                                                                                                                                                                                                                                              |
| <b>Step 5</b> | <pre>encapsulation {mpls   l2tpv3}</pre> <p><b>Example:</b><br/>Router(config-pw)# encapsulation mpls</p>                                | Specifies the tunneling encapsulation, which is either <b>mpls</b> or <b>l2tpv3</b> .                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 6</b> | <pre>interworking {ethernet   ip}   vlan}</pre> <p><b>Example:</b><br/>Router(config-pw)# interworking ip</p>                            | <p>Specifies the type of pseudowire and the type of traffic that can flow across it.</p> <p><b>Note</b> On the Cisco 12000 series Internet router, Ethernet (bridged) interworking is not supported for L2TPv3.<br/>After you configure the L2TPv3 tunnel encapsulation for the pseudowire using the <b>encapsulation l2tpv3</b> command, you cannot enter the <b>interworking ethernet</b> command.</p>                                 |

## Verifying the L2VPN Interworking Configuration

To verify the L2VPN Interworking configuration, you can use the following commands.

### SUMMARY STEPS

1. **enable**
1. **show l2tun session all**
2. **show arp**
3. **ping**
4. **show l2tun session interworking**
5. **show mpls l2transport vc detail**

### DETAILED STEPS

**Step 1**    **enable**

Enables privileged EXEC mode. Enter your password if prompted.

### Step 2 **show l2tun session all** (L2TPv3 only)

For L2TPv3, you can verify the L2VPN Interworking configuration using the **show l2tun session all** command on the PE routers.

In the following example, the interworking type is shown in bold.

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router# show l2tun session all  Session Information Total tunnels 1 sessions 1  Session id 15736 is up, tunnel id 35411 Call serial number is 4035100045 Remote tunnel name is PE2   Internet address is 10.9.9.9   Session is L2TP signalled   Session state is established, time since change 1d22h   16 Packets sent, 16 received   1518 Bytes sent, 1230 received   Receive packets dropped:     out-of-order:      0     total:             0   Send packets dropped:     exceeded session MTU: 0     total:             0   Session vcid is 123   Session Layer 2 circuit, type is Ethernet,   name is FastEthernet1/1/0   Circuit state is UP   Remote session id is 26570, remote tunnel   id 46882   DF bit off, ToS reflect disabled, ToS value   0, TTL value 255   No session cookie information available   FS cached header information:     encaps size = 24 bytes     00000000 00000000 00000000 00000000     00000000 00000000   Sequencing is off</pre> | <pre>Router# show l2tun session all  Session Information Total tunnels 1 sessions 1  Session id 26570 is up, tunnel id 46882 Call serial number is 4035100045 Remote tunnel name is PE1   Internet address is 10.8.8.8   Session is L2TP signalled   Session state is established, time since change 1d22h   16 Packets sent, 16 received   1230 Bytes sent, 1230 received   Receive packets dropped:     out-of-order:      0     total:             0   Send packets dropped:     exceeded session MTU: 0     total:             0   Session vcid is 123   Session Layer 2 circuit, type is Ethernet Vlan, name is   FastEthernet2/0.1:10   Circuit state is UP, <b>interworking type is Ethernet</b>   Remote session id is 15736, remote tunnel id 35411   DF bit off, ToS reflect disabled, ToS value 0, TTL   value 255   No session cookie information available   FS cached header information:     encaps size = 24 bytes     00000000 00000000 00000000 00000000     00000000 00000000   Sequencing is off</pre> |

### Step 3 **show arp**

You can issue the **show arp** command between the CE routers to ensure that data is being sent:

```
Router# show arp
```

| Protocol | Address  | Age (min) | Hardware Addr  | Type | Interface       |
|----------|----------|-----------|----------------|------|-----------------|
| Internet | 10.1.1.5 | 134       | 0005.0032.0854 | ARPA | FastEthernet0/0 |
| Internet | 10.1.1.7 | -         | 0005.0032.0000 | ARPA | FastEthernet0/0 |

### Step 4 **ping**

You can issue the **ping** command between the CE routers to ensure that data is being sent:

```
Router# ping 10.1.1.5
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

**Step 5 show l2tun session interworking (L2TPv3 only)**

For L2TPv3, you can verify that the interworking type is correctly set using the **show l2tun session interworking** command. Enter the command on the PE routers that are performing the interworking translation.

- In Example 1, the PE router performs the raw Ethernet translation. The command output displays the interworking type with a dash (-).
- In Example 2, the PE router performs the Ethernet VLAN translation. The command output displays the interworking type as ETH.

**Example 1 Command Output for Raw Ethernet Translation**

```
Router# show l2tun session interworking

Session Information Total tunnels 1 sessions 1

LocID      TunID      Peer-address      Type IWrk Username, Intf/Vcid, Circuit
15736      35411      10.9.9.9          ETH  -   123,      Fa1/1/0
```

**Example 2 Command Output for Ethernet VLAN Translation**

```
Router# show l2tun session interworking

Session Information Total tunnels 1 sessions 1

LocID      TunID      Peer-address      Type IWrk Username, Intf/Vcid, Circuit
26570      46882      10.8.8.8          VLAN ETH  123,      Fa2/0.1:10
```

**Step 6 show mpls l2transport vc detail (AToM only)**

You can verify the AToM configuration by using the **show mpls l2transport vc detail** command. In the following example, the interworking type is shown in bold.

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router# show mpls l2transport vc detail  Local interface: Fa1/1/0 up, line protocol up, Ethernet up   Destination address: 10.9.9.9, VC ID: 123, VC status: up     Preferred path: not configured     Default path: active     Tunnel label: 17, next hop 10.1.1.3     Output interface: Fa4/0/0, imposed label stack {17 20}   Create time: 01:43:50, last status change time: 01:43:33   Signaling protocol: LDP, peer 10.9.9.9:0 up     MPLS VC labels: local 16, remote 20     Group ID: local 0, remote 0     MTU: local 1500, remote 1500     Remote interface description: Sequencing: receive disabled, send disabled VC statistics:   packet totals: receive 15, send 4184   byte totals:   receive 1830, send 309248   packet drops:  receive 0, send 0</pre> | <pre>Router# show mpls l2transport vc detail  Local interface: Fa2/0.3 up, line protocol up, Eth VLAN 10 up   MPLS VC type is Ethernet, <b>interworking type is Ethernet</b>   Destination address: 10.8.8.8, VC ID: 123, VC status: up     Preferred path: not configured     Default path: active     Tunnel label: 16, next hop 10.1.1.3     Output interface: Fa6/0, imposed label stack {16 16}   Create time: 00:00:26, last status change time: 00:00:06   Signaling protocol: LDP, peer 10.8.8.8:0 up     MPLS VC labels: local 20, remote 16     Group ID: local 0, remote 0     MTU: local 1500, remote 1500     Remote interface description: Sequencing: receive disabled, send disabled VC statistics:   packet totals: receive 5, send 0   byte totals:   receive 340, send 0   packet drops:  receive 0, send 0</pre> |

## Configuring L2VPN Interworking: VLAN Enable/Disable Option for AToM

You can specify the Ethernet VLAN (type 4) by issuing the **interworking vlan** command in pseudowire-class configuration mode. This allows the VLAN ID to be included as part of the Ethernet frame. In releases previous to Cisco IOS Release 12.2(52)SE and Cisco IOS Release 12.2(33)SRE, the only way to achieve VLAN encapsulation is to ensure the CE router is connected to the PE router through an Ethernet link.

### Restrictions

In Cisco IOS Release 12.2(52)SE and Cisco IOS Release 12.2(33)SRE, the **encapsulation** command supports only the **mpls** keyword. The **l2tpv3** keyword is not supported. The **interworking** command supports only the **ethernet** and **vlan** keywords. The **ip** keyword is not supported.

### Prerequisites

For complete instructions on configuring AToM, see [Any Transport over MPLS](#).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation** { **mpls** | **l2tpv3** }
5. **interworking** { **ethernet** | **ip** | **vlan** }
6. **end**
7. **show mpls l2transport vc** [**vcid** *vc-id* | **vcid** *vc-id-min* *vc-id-max*] [**interface** *type number* [*local-circuit-id*]] [**destination** *ip-address* | *name*] [**detail**]

### DETAILED STEPS

|        | Command or Action                                          | Purpose                                                                                                     |
|--------|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                              | Enables privileged EXEC mode.                                                                               |
|        | <b>Example:</b><br>Router> enable                          | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                        |
| Step 2 | <b>configure terminal</b>                                  | Enters global configuration mode.                                                                           |
|        | <b>Example:</b><br>Router# configure terminal              |                                                                                                             |
| Step 3 | <b>pseudowire-class</b> <i>name</i>                        | Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode. |
|        | <b>Example:</b><br>Router(config)# pseudowire-class class1 |                                                                                                             |

|               | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <b>encapsulation</b> { <b>mpls</b>   <b>l2tpv3</b> }<br><br><b>Example:</b><br>Router(config-pw)# encapsulation mpls                                                                                                                                                                                                       | Specifies the tunneling encapsulation, which is either <b>mpls</b> or <b>l2tpv3</b> . <ul style="list-style-type: none"> <li>For the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature, only MPLS encapsulation is supported.</li> </ul> |
| <b>Step 5</b> | <b>interworking</b> { <b>ethernet</b>   <b>ip</b>   <b>vlan</b> }<br><br><b>Example:</b><br>Router(config-pw)# interworking vlan                                                                                                                                                                                           | Specifies the type of pseudowire and the type of traffic that can flow across it. <ul style="list-style-type: none"> <li>For the L2VPN Interworking: VLAN Enable/Disable Option for AToM feature, specify the <b>vlan</b> keyword.</li> </ul>          |
| <b>Step 6</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-pw)# end                                                                                                                                                                                                                                                                | Exits pseudowire class configuration mode and enters privileged EXEC mode.                                                                                                                                                                             |
| <b>Step 7</b> | <b>show mpls l2transport vc</b> [ <b>vcid</b> <b>vc-id</b>   <b>vcid</b> <b>vc-id-min</b> <b>vc-id-max</b> ] [ <b>interface</b> <i>type number</i> [ <b>local-circuit-id</b> ]] [ <b>destination</b> <i>ip-address</i>   <i>name</i> ] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show mpls l2transport vc detail | Displays information about AToM VCs.                                                                                                                                                                                                                   |

## Examples

When the pseudowire on an interface is different from the VC type, the interworking type is displayed in the **show mpls l2transport vc detail** command output. In the following example, the pseudowire is configured on an Ethernet port and VLAN interworking is configured in the pseudowire class. The relevant output is shown in bold:

```

PE1# show mpls l2 vc 34 detail

Local interface: Et0/1 up, line protocol up, Ethernet up
MPLS VC type is Ethernet, interworking type is Eth VLAN
Destination address: 10.1.1.2, VC ID: 34, VC status: down
Output interface: if-?(0), imposed label stack {}
Preferred path: not configured
Default path: no route
No adjacency
Create time: 00:00:13, last status change time: 00:00:13
Signaling protocol: LDP, peer unknown
Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.2
Status TLV support (local/remote)   : enabled/None (no remote binding)
LDP route watch                     : enabled
Label/status state machine           : local standby, AC-ready, LnuRnd
Last local dataplane status rcvd: No fault
Last local SSS circuit status rcvd: No fault
Last local SSS circuit status sent: Not sent
Last local LDP TLV status sent: None
Last remote LDP TLV status rcvd: None (no remote binding)
Last remote LDP ADJ status rcvd: None (no remote binding)
MPLS VC labels: local 2003, remote unassigned
Group ID: local 0, remote unknown
MTU: local 1500, remote unknown
Remote interface description:
Sequencing: receive disabled, send disabled

```



```

VC statistics:
  packet totals: receive 0, send 0
  byte totals:   receive 0, send 0
  packet drops:  receive 0, seq error 0, send 0

```

## Configuration Examples for L2VPN Interworking

The following sections show examples of L2VPN Interworking:

- [Ethernet to VLAN over L2TPV3 \(Bridged\): Example, page 21](#)
- [Ethernet to VLAN over AToM \(Bridged\): Example, page 22](#)
- [Frame Relay to VLAN over L2TPV3 \(Routed\): Example, page 22](#)
- [Frame Relay to VLAN over AToM \(Routed\): Example, page 23](#)
- [Frame Relay to ATM AAL5 over AToM \(Routed\): Example, page 24](#)
- [VLAN to ATM AAL5 over AToM \(Bridged\): Example, page 25](#)
- [Frame Relay to PPP over L2TPv3 \(Routed\): Example, page 26](#)
- [Frame Relay to PPP over AToM \(Routed\): Example, page 27](#)
- [Ethernet/VLAN to PPP over AToM \(Routed\): Example, page 28](#)
- [Additional References, page 28](#)

### Ethernet to VLAN over L2TPV3 (Bridged): Example

The following example shows the configuration of Ethernet to VLAN over L2TPv3:

| PE1                                                                                                                                                                                                                                                                                                                                                                               | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef ! l2tp-class interworking-class authentication hostname PE1 password 0 lab ! pseudowire-class inter-ether-vlan encapsulation l2tpv3 interworking ethernet protocol l2tpv3 interworking-class ip local interface Loopback0 ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/0 xconnect 10.9.9.9 1 pw-class inter-ether-vlan </pre> | <pre> ip cef ! l2tp-class interworking-class authentication hostname PE2 password 0 lab ! pseudowire-class inter-ether-vlan encapsulation l2tpv3 interworking ethernet protocol l2tpv3 interworking-class ip local interface Loopback0 ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0 no ip address ! interface FastEthernet0/0.3 encapsulation dot1Q 10 xconnect 10.8.8.8 1 pw-class inter-ether-vlan </pre> |

## Ethernet to VLAN over AToM (Bridged): Example

The following example shows the configuration of Ethernet to VLAN over AToM:

| PE1                                                                                                                                                                                                                                                                                                                         | PE2                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! pseudowire-class atom-eth-iw   encapsulation mpls   interworking ethernet ! interface Loopback0 ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/0.1   encapsulation dot1q 100   xconnect 10.9.9.9 123 pw-class atom-eth-iw </pre> | <pre> ip cef ! mpls label protocol ldp mpls ldp router-id Loopback0 force ! pseudowire-class atom   encapsulation mpls ! interface Loopback0 ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0   no ip address ! interface FastEthernet1/0   xconnect 10.9.9.9 123 pw-class atom </pre> |

## Frame Relay to VLAN over L2TPV3 (Routed): Example

The following example shows the configuration of Frame Relay to VLAN over L2TPv3:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> configure terminal ip cef frame-relay switching ! ! interface loopback 0 ip address 10.8.8.8 255.255.255.255 no shutdown ! pseudowire-class ip   encapsulation l2tpv3   interworking ip   ip local interface loopback0 ! interface POS1/0   encapsulation frame-relay   clock source internal   logging event dlci-status-change   no shutdown   no fair-queue ! connect fr-vlan POS1/0 206 l2transport   xconnect 10.9.9.9 6 pw-class ip ! router ospf 10   network 10.0.0.2 0.0.0.0 area 0   network 10.8.8.8 0.0.0.0 area 0 </pre> | <pre> configure terminal ip routing ip cef frame-relay switching ! interface loopback 0 ip address 10.9.9.9 255.255.255.255 no shutdown ! pseudowire-class ip   encapsulation l2tpv3   interworking ip   ip local interface loopback0 ! interface FastEthernet1/0/1   speed 10   no shutdown ! interface FastEthernet1/0/1.6   encapsulation dot1Q 6   xconnect 10.8.8.8 6 pw-class ip   no shutdown ! router ospf 10   network 10.0.0.2 0.0.0.0 area 0   network 10.9.9.9 0.0.0.0 area 0 </pre> |

## Frame Relay to VLAN over AToM (Routed): Example

The following example shows the configuration of Frame Relay to VLAN over AToM:

| PE1                                                                                                                                                                                                                                                                                                                                              | PE2                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>configure terminal ip cef frame-relay switching ! mpls label protocol ldp mpls ldp router-id loopback0 mpls ip ! pseudowire-class atom   encapsulation mpls   interworking ip ! interface loopback 0   ip address 10.8.8.8 255.255.255.255   no shutdown ! connect fr-vlan POS1/0 206 l2transport   xconnect 10.9.9.9 6 pw-class atom</pre> | <pre>configure terminal ip routing ip cef frame-relay switching ! mpls label protocol ldp mpls ldp router-id loopback0 mpls ip ! pseudowire-class atom   encapsulation mpls   interworking ip ! interface loopback 0   ip address 10.9.9.9 255.255.255.255   no shutdown ! interface FastEthernet1/0/1.6   encapsulation dot1Q 6   xconnect 10.8.8.8 6 pw-class atom   no shutdown</pre> |

## Frame Relay to ATM AAL5 over AToM (Routed): Example


**Note**

Frame Relay to ATM AAL5 is available only with AToM in IP mode.

The following example shows the configuration of Frame Relay to ATM AAL5 over AToM:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef frame-relay switching mpls ip mpls label protocol ldp mpls ldp router-id loopback0 force pseudowire-class fratmip encapsulation mpls interworking ip interface Loopback0 ip address 10.33.33.33 255.255.255.255 interface serial 2/0 encapsulation frame-relay ietf frame-relay intf-type dce connect fr-eth serial 2/0 100 l2transport xconnect 10.22.22.22 333 pw-class fratmip interface POS1/0 ip address 10.1.7.3 255.255.255.0 crc 32 clock source internal mpls ip mpls label protocol ldp router ospf 10 passive-interface Loopback0 network 10.33.33.33 0.0.0.0 area 10 network 10.1.7.0 0.0.0.255 area 10 </pre> | <pre> ip cef mpls ip mpls label protocol ldp mpls ldp router-id loopback0 force pseudowire-class fratmip encapsulation mpls interworking ip interface Loopback0 ip address 10.22.22.22 255.255.255.255 interface ATM 2/0 pvc 0/203 l2transport encapsulation aa5snap xconnect 10.33.33.33 333 pw-class fratmip interface POS1/0 ip address 10.1.1.2 255.255.255.0 crc 32 clock source internal mpls ip mpls label protocol ldp router ospf 10 passive-interface Loopback0 network 10.22.22.22 0.0.0.0 area 10 network 10.1.1.0 0.0.0.255 area 10 </pre> |

## VLAN to ATM AAL5 over AToM (Bridged): Example

The following example shows the configuration of VLAN to ATM AAL5 over AToM:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! pseudowire-class inter-ether encapsulation mpls interworking ethernet ! interface Loopback0  ip address 10.8.8.8 255.255.255.255 ! interface ATM1/0.1 point-to-point  pvc 0/100 l2transport  encapsulation aal5snap  xconnect 10.9.9.9 123 pw-class inter-ether ! interface FastEthernet1/0  xconnect 10.9.9.9 1 pw-class inter-ether ! router ospf 10  log-adjacency-changes  network 10.8.8.8 0.0.0.0 area 0  network 10.1.1.1 0.0.0.0 area 0 </pre> | <pre> ip cef ! mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 ! pseudowire-class inter-ether  encapsulation mpls  interworking ethernet ! interface Loopback0  ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet0/0  no ip address ! interface FastEthernet0/0.1  encapsulation dot1Q 10  xconnect 10.8.8.8 123 pw-class inter-ether ! router ospf 10  log-adjacency-changes  network 10.9.9.9 0.0.0.0 area 0  network 10.1.1.2 0.0.0.0 area 0 </pre> |

## Frame Relay to PPP over L2TPv3 (Routed): Example

The following example shows the configuration of Frame Relay to PPP over L2TPv3:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                          | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef ip routing ! ! ! pseudowire-class ppp-fr encapsulation l2tpv3 interworking ip ip local interface Loopback0 ! interface Loopback0  ip address 10.1.1.1 255.255.255.255 ! interface FastEthernet1/0/0  ip address 10.16.1.1 255.255.255.0 ! interface Serial3/0/0 no ip address encapsulation ppp ppp authentication chap ! ip route 10.0.0.0 255.0.0.0 10.16.1.2 ! xconnect 10.2.2.2 1 pw-class ppp-fr ppp ipcp address proxy 10.65.32.14 </pre> | <pre> ip cef ip routing ! frame-relay switching ! pseudowire-class ppp-fr encapsulation l2tpv3 interworking ip ip local interface Loopback0 ! interface Loopback0  ip address 10.2.2.2 255.255.255.255 ! interface FastEthernet1/0/0  ip address 10.16.2.1 255.255.255.0 ! interface Serial3/0/0 no ip address encapsulation frame-relay frame-relay intf-type dce ! ip route 10.0.0.0 255.0.0.0 10.16.2.2 ! connect ppp-fr Serial3/0/0 100 l2transport xconnect 10.1.1.1 100 pw-class ppp-fr </pre> |

## Frame Relay to PPP over AToM (Routed): Example

The following example shows the configuration of Frame Relay to PPP over AToM:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip cef ip routing mpls label protocol ldp mpls ldp router-id loopback0 force ! ! ! pseudowire-class ppp-fr encapsulation mpls interworking ip ip local interface Loopback0 ! interface Loopback0  ip address 10.1.1.1 255.255.255.255 ! interface FastEthernet1/0/0  ip address 10.16.1.1 255.255.255.0 mpls ip label protocol ldp ! interface Serial3/0/0  no ip address  encapsulation ppp  ppp authentication chap  xconnect 10.2.2.2 1 pw-class ppp-fr  ppp ipcp address proxy 10.65.32.14 ! ip route 10.0.0.0 255.0.0.0 10.16.1.2 </pre> | <pre> ip cef ip routing mpls label protocol ldp mpls ldp router-id loopback0 force ! ! frame-relay switching ! pseudowire-class ppp-fr encapsulation mpls interworking ip ip local interface Loopback0 ! interface Loopback0  ip address 10.2.2.2 255.255.255.255 ! interface FastEthernet1/0/0  ip address 10.16.2.1 255.255.255.0 mpls ip mpls label protocol ldp ! interface Serial3/0/0  no ip address  encapsulation frame-relay  frame-relay intf-type dce ! ip route 10.0.0.0 255.0.0.0 10.16.2.2 ! connect ppp-fr Serial3/0/0 100 l2transport  xconnect 10.1.1.1 100 pw-class ppp-fr </pre> |

## Ethernet/VLAN to PPP over AToM (Routed): Example

The following example shows the configuration of Ethernet VLAN to PPP over AToM:

| PE1                                                                                                                                                                                                                                                                                                                                                                                                                 | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> configure terminal mpls label protocol ldp mpls ldp router-id Loopback0 mpls ip ! pseudowire-class ppp-ether  encapsulation mpls  interworking ip ! interface Loopback0  ip address 10.8.8.8 255.255.255.255  no shutdown ! interface POS2/0/1  no ip address  encapsulation ppp  no peer default ip address  ppp ipcp address proxy 10.10.10.1  xconnect 10.9.9.9 300 pw-class ppp-ether  no shutdown </pre> | <pre> configure terminal mpls label protocol ldp mpls ldp router-id Loopback0 mpls ip ! pseudowire-class ppp-ether  encapsulation mpls  interworking ip ! interface Loopback0  ip address 10.9.9.9 255.255.255.255  no shutdown ! interface vlan300  mtu 4470  no ip address  xconnect 10.8.8.8 300 pw-class ppp-ether  no shutdown ! interface GigabitEthernet6/2  switchport  switchport trunk encapsulation dot1q  switchport trunk allowed vlan 300  switchport mode trunk  no shutdown </pre> |

## Additional References

The following sections provide references related to the L2VPN Interworking feature.

## Related Documents

| Related Topic                               | Document Title                                                                                                                                                                                                          |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Layer 2 Tunnel Protocol Version 3           | <a href="#">Layer 2 Tunnel Protocol Version 3</a>                                                                                                                                                                       |
| Any Transport over MPLS                     | <a href="#">Any Transport over MPLS</a>                                                                                                                                                                                 |
| Cisco 12000 series routers hardware support | <a href="#">Cross-Platform Release Notes for Cisco IOS Release 12.0S.</a>                                                                                                                                               |
| Cisco 7600 series routers hardware support  | <ul style="list-style-type: none"> <li><a href="#">Cisco 7600 Series Routers Documentation Roadmap</a></li> <li><a href="#">Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers</a></li> </ul> |
| Cisco 3270 series routers hardware support  | <a href="#">Cisco IOS Software Releases 12.2SE Release Notes</a>                                                                                                                                                        |



## Standards

| Standards                                   | Title                                                                                  |
|---------------------------------------------|----------------------------------------------------------------------------------------|
| draft-ietf-l2tpext-l2tp-base-03.txt         | <i>Layer Two Tunneling Protocol (Version 3) 'L2TPv3'</i>                               |
| draft-martini-l2circuit-trans-mpls-09.txt   | <i>Transport of Layer 2 Frames Over MPLS</i>                                           |
| draft-ietf-pwe3-frame-relay-03.txt.         | <i>Encapsulation Methods for Transport of Frame Relay over MPLS Networks</i>           |
| draft-martini-l2circuit-encap-mpls-04.txt.  | <i>Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks</i> |
| draft-ietf-pwe3-ethernet-encap-08.txt.      | <i>Encapsulation Methods for Transport of Ethernet over MPLS Networks</i>              |
| draft-ietf-pwe3-hdlc-ppp-encap-mpls-03.txt. | <i>Encapsulation Methods for Transport of PPP/HDLC over MPLS Networks</i>              |
| draft-ietf-ppvpn-l2vpn-00.txt.              | <i>An Architecture for L2VPNs</i>                                                      |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for L2VPN Interworking

Table 6 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 6 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 6** Feature Information for L2VPN Interworking

| Feature Name       | Releases                                                                                                                                 | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2VPN Interworking | 12.0(26)S<br>12.0(30)S<br>12.0(32)S<br>12.0(32)SY<br>12.2(33)SRA<br>12.4(11)T<br>12.2(33)SXH<br>12.2(33)SRD<br>12.2(52)SE<br>12.2(33)SRE | <p>This feature allows disparate attachment circuits to be connected. An interworking function facilitates the translation between the different Layer 2 encapsulations.</p> <p>This feature was introduced in Cisco IOS Release 12.0(26)S.</p> <p>In Cisco IOS Release 12.0(30)S, support was added for Cisco 12000 series Internet routers.</p> <p>In Cisco IOS Release 12.0(32)S, support was added on Engine 5 line cards (SIP-401, SIP-501, SIP-600, and SIP-601) in Cisco 12000 series routers for the following four transport types:</p> <ul style="list-style-type: none"> <li>• Ethernet/VLAN to Frame Relay Interworking</li> <li>• Ethernet/VLAN to ATM AAL5 Interworking</li> <li>• Ethernet to VLAN Interworking</li> <li>• Frame Relay to ATM AAL5 Interworking</li> </ul> <p>On the Cisco 12000 series Internet router, support was added for IP Services Engine (ISE) and Engine 5 line cards that are configured for L2TPv3 tunneling (see <a href="#">Layer 2 Tunnel Protocol Version 3</a>).</p> <p>In Cisco IOS Release 12.2(33)SRA, support was added for the Cisco 7600 series routers.</p> <p>In Cisco IOS Release 12.4(11)T, support was added for the following transport types:</p> <ul style="list-style-type: none"> <li>• Ethernet to VLAN Interworking</li> <li>• Ethernet/VLAN to Frame Relay Interworking</li> </ul> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>In Cisco IOS Release 12.2(33)SRD, support for routed and bridged interworking on SIP-400 was added for the Cisco 7600 series routers.</p> <p>In Cisco IOS Release 12.2(52)SE, the L2VPN Interworking: VLAN Enable/Disable Option for ATOM feature was added for the Cisco 3750 Metro switch.</p> <p>In Cisco IOS Release 12.2(33)SRE, the L2VPN Interworking: VLAN Enable/Disable Option for ATOM feature was added for the Cisco 7600 series router.</p> <p>The following commands were introduced or modified: <b>interworking</b></p> |

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

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

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

© 2003-2009 Cisco Systems, Inc. All rights reserved.





# L2VPN Pseudowire Redundancy

---

**First Published: April 20, 2005**

**Last Updated: November 20, 2009**

The L2VPN Pseudowire Redundancy feature lets you configure your network to detect a failure in the network and reroute the Layer 2 (L2) service to another endpoint that can continue to provide service. This feature provides the ability to recover from a failure either of the remote provider edge (PE) router or of the link between the PE and customer edge (CE) routers.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for L2VPN Pseudowire Redundancy” section on page 14](#).

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

## Contents

- [Prerequisites for L2VPN Pseudowire Redundancy, page 2](#)
- [Restrictions for L2VPN Pseudowire Redundancy, page 2](#)
- [Information About L2VPN Pseudowire Redundancy, page 3](#)
- [How to Configure L2VPN Pseudowire Redundancy, page 5](#)
- [Configuration Examples for L2VPN Pseudowire Redundancy, page 10](#)
- [Additional References, page 12](#)
- [Command Reference, page 13](#)
- [Feature Information for L2VPN Pseudowire Redundancy, page 14](#)



---

**Americas Headquarters:**

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

## Prerequisites for L2VPN Pseudowire Redundancy

- This feature module requires that you understand how to configure basic L2 virtual private networks (VPNs). You can find that information in the following documents:
  - *Any Transport over MPLS*
  - *L2 VPN Interworking*
- The L2VPN Pseudowire Redundancy feature requires that the following mechanisms be in place to enable you to detect a failure in the network:
  - Label-switched paths (LSP) Ping/Traceroute and Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV)
  - Local Management Interface (LMI)
  - Operation, Administration, and Maintenance (OAM)

## Restrictions for L2VPN Pseudowire Redundancy

### General Restrictions

- The primary and backup pseudowires must run the same type of transport service. The primary and backup pseudowires must be configured with AToM.
- Only static, on-box provisioning is supported.
- If you use L2VPN Pseudowire Redundancy with L2VPN Interworking, the interworking method must be the same for the primary and backup pseudowires.
- Setting the experimental (EXP) bit on the Multiprotocol Label Switching (MPLS) pseudowire is supported.
- Different pseudowire encapsulation types on the MPLS pseudowire are not supported.
- The **mpls l2transport route** command is not supported. Use the **xconnect** command instead.
- The ability to have the backup pseudowire fully operational at the same time that the primary pseudowire is operational is not supported. The backup pseudowire becomes active only after the primary pseudowire fails.
- The AToM VCCV feature is supported only on the active pseudowire.
- More than one backup pseudowire is not supported.

### Restrictions for Layer 2 Tunnel Protocol Version 3 (L2TPv3) Xconnect Configurations

- Interworking is not supported.
- Local switching backup by pseudowire redundancy is not supported.
- PPP, HDLC, and Frame-Relay attachment circuit (AC) types of L2TPv3 pseudowire redundancy are not supported.
- For the edge interface, only the Cisco 7600 series SPA Interface Processor-400 (SIP-400) linecard with the following shared port adapters (SPAs) is supported:
  - Cisco 2-Port Gigabit Ethernet Shared Port Adapter (SPA-2X1GE)
  - Cisco 2-Port Gigabit Ethernet Shared Port Adapter, Version 2 (SPA-2X1GE-V2)
  - Cisco 5-Port Gigabit Ethernet Shared Port Adapter, Version 2 (SPA-5X1GE-V2)
  - Cisco 10-Port Gigabit Ethernet Shared Port Adapter, Version 2 (SPA-10X1GE-V2)



Cisco 2-Port OC3c/STM1c ATM Shared Port Adapter (SPA-2XOC3-ATM)  
Cisco 4-Port OC3c/STM1c ATM Shared Port Adapter (SPA-4XOC3-ATM)  
Cisco 1-Port OC12c/STM4c ATM Shared Port Adapter (SPA-1XOC12-ATM)  
Cisco 1-Port OC-48c/STM-16 ATM Shared Port Adapter (SPA-1XOC48-ATM)

## Information About L2VPN Pseudowire Redundancy

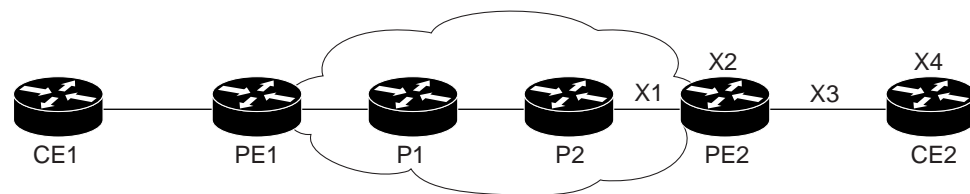
Make sure that you understand the following concept before configuring the L2VPN Pseudowire Redundancy feature:

- [Introduction to L2VPN Pseudowire Redundancy](#), page 3

## Introduction to L2VPN Pseudowire Redundancy

L2VPNs can provide pseudowire resiliency through their routing protocols. When connectivity between end-to-end PE routers fails, an alternative path to the directed LDP session and the user data can take over. However, there are some parts of the network where this rerouting mechanism does not protect against interruptions in service. [Figure 1](#) shows those parts of the network that are vulnerable to an interruption in service.

**Figure 1**      *Points of Potential Failure in an L2VPN Network*



X1 = End-to-end routing failure  
X2 = PE hardware or software failure  
X3 = Attachment circuit failure from a line break  
X4 = CE hardware or software failure

135057

The L2VPN Pseudowire Redundancy feature provides the ability to ensure that the CE2 router in [Figure 1](#) can always maintain network connectivity, even if one or all the failures in the figure occur.

The L2VPN Pseudowire Redundancy feature enables you to set up backup pseudowires. You can configure the network with redundant pseudowires (PWs) and redundant network elements, which are shown in [Figure 2](#), [Figure 3](#), and [Figure 4](#).

Figure 2 shows a network with redundant pseudowires and redundant attachment circuits.

**Figure 2** L2VPN Network with Redundant PWs and Attachment Circuits

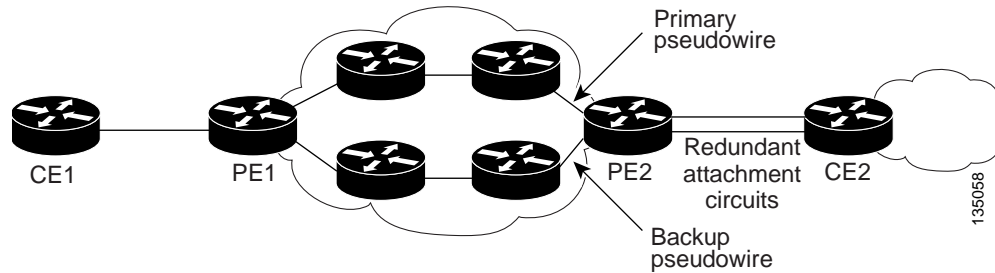


Figure 3 shows a network with redundant pseudowires, attachment circuits, and CE routers.

**Figure 3** L2VPN Network with Redundant PWs, Attachment Circuits, and CE Routers

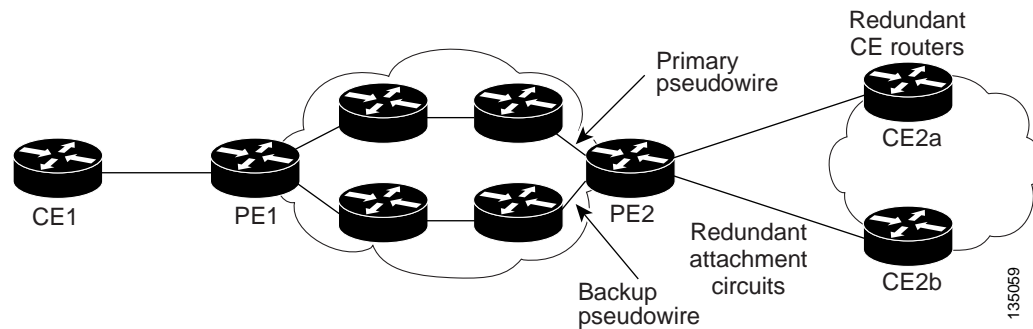
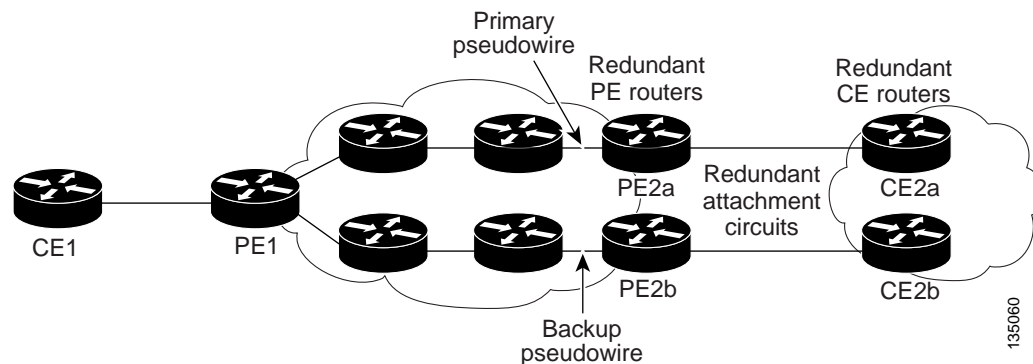


Figure 4 shows a network with redundant pseudowires, attachment circuits, CE routers, and PE routers.

**Figure 4** L2VPN Network with Redundant PWs, Attachment Circuits, CE Routers, and PE Routers



# How to Configure L2VPN Pseudowire Redundancy

The L2VPN Pseudowire Redundancy feature enables you to configure a backup pseudowire in case the primary pseudowire fails. When the primary pseudowire fails, the PE router can switch to the backup pseudowire. You can have the primary pseudowire resume operation after it comes back up.

The default Label Distribution Protocol (LDP) session hold-down timer will enable the software to detect failures in about 180 seconds. That time can be configured so that the software can detect failures more quickly. See the **mpls ldp holdtime** command for more information.

The following sections explain how to configure the L2VPN Pseudowire Redundancy feature:

- [Configuring the Pseudowire, page 5](#) (required)
- [Configuring L2VPN Pseudowire Redundancy, page 6](#) (required)
- [Forcing a Manual Switchover to the Backup Pseudowire VC, page 8](#) (optional)
- [Verifying the L2VPN Pseudowire Redundancy Configuration, page 8](#) (optional)

## Configuring the Pseudowire

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You set up the connection, called a pseudowire, between the routers.

The pseudowire-class configuration group specifies the characteristics of the tunneling mechanism, which are:

- Encapsulation type
- Control protocol
- Payload-specific options

You must specify the **encapsulation mpls** command as part of the pseudowire class for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **xconnect** command, you receive the following error:

```
% Incomplete command.
```

Perform this task to configure a pseudowire class.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**
5. **interworking** {*ethernet* | *ip*}

## DETAILED STEPS

|        | Command or Action                                                                                      | Purpose                                                                                                           |
|--------|--------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                         | Enters global configuration mode.                                                                                 |
| Step 3 | <b>pseudowire-class</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom    | Establishes a pseudowire class with a name that you specify. Enters pseudowire class configuration mode.          |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw-class)# encapsulation mpls        | Specifies the tunneling encapsulation. For AToM, the encapsulation type is <b>mpls</b> .                          |
| Step 5 | <b>interworking {ethernet   ip}</b><br><br><b>Example:</b><br>Router(config-pw-class)# interworking ip | (Optional) Enables the translation between the different Layer 2 encapsulations.                                  |

## Configuring L2VPN Pseudowire Redundancy

Use the following steps to configure the L2VPN Pseudowire Redundancy feature.

## Prerequisites

For each transport type, the **xconnect** command is configured slightly differently. The following configuration steps use Ethernet VLAN over MPLS, which is configured in subinterface configuration mode. See *Any Transport over MPLS* to determine how to configure the **xconnect** command for other transport types.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *gigabitethernet slot/subslot/interface.subinterface*
4. **encapsulation dot1q** *vlan-id*
5. **xconnect** *peer-router-id vcid {encapsulation mpls | pw-class pw-class-name}*
6. **backup peer** *peer-router-ip-addr vcid [pw-class pw-class-name]*
7. **backup delay** *enable-delay {disable-delay | never}*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>gigabitethernet</i> <i>slot/subslot/interface.subinterface</i><br><br><b>Example:</b><br>Router(config)# interface gigabitethernet0/0/0.1                                              | Specifies the Gigabit Ethernet subinterface and enters subinterface configuration mode.<br><br>Make sure that the subinterface on the adjoining CE router is on the same VLAN as this PE router.                                                                                                                                                                                                                        |
| Step 4 | <b>encapsulation dot1q</b> <i>vlan-id</i><br><br><b>Example:</b><br>Router(config-subif)# encapsulation dot1q 100                                                                                          | Enables the subinterface to accept 802.1Q VLAN packets.<br><br>The subinterfaces between the CE and PE routers that are running Ethernet over MPLS must be in the same subnet. All other subinterfaces and backbone routers do not.                                                                                                                                                                                     |
| Step 5 | <b>xconnect</b> <i>peer-router-id</i> <i>vcid</i> { <b>encapsulation mpls</b>   <b>pw-class</b> <i>pw-class-name</i> }<br><br><b>Example:</b><br>Router(config-subif)# xconnect 10.0.0.1 123 pw-class atom | Binds the attachment circuit to a pseudowire VC.<br><br>The syntax for this command is the same as for all other Layer 2 transports.<br><br>Enters xconnect configuration mode.                                                                                                                                                                                                                                         |
| Step 6 | <b>backup peer</b> <i>peer-router-ip-addr</i> <i>vcid</i> [ <b>pw-class</b> <i>pw-class-name</i> ]<br><br><b>Example:</b><br>Router(config-if-xconn)# backup peer 10.0.0.3 125 pw-class atom               | Specifies a redundant peer for the pseudowire VC.<br><br>The pseudowire class name must match the name you specified when you created the pseudowire class, but you can use a different pw-class in the <b>backup peer</b> command than the name that you used in the primary <b>xconnect</b> command.                                                                                                                  |
| Step 7 | <b>backup delay</b> <i>enable-delay</i> { <i>disable-delay</i>   <b>never</b> }<br><br><b>Example:</b><br>Router(config-if-xconn)# backup delay 5 never                                                    | Specifies how long (in seconds) the backup pseudowire VC should wait to take over after the primary pseudowire VC goes down. The range is 0 to 180.<br><br>Specifies how long the primary pseudowire should wait after it becomes active to take over for the backup pseudowire VC. The range is 0 to 180 seconds. If you specify the <b>never keyword</b> , the primary pseudowire VC never takes over for the backup. |

## Forcing a Manual Switchover to the Backup Pseudowire VC

To force the router switch over to the backup or primary pseudowire, you can enter the **xconnect backup force switchover** command in privileged EXEC mode. You can specify either the interface of the primary attachment circuit (AC) to switch to or the IP-address and VC ID of the peer router.

A manual switchover can be made only if the interface or peer specified in the command is actually available and the xconnect will move to the fully active state when the command is entered.

### SUMMARY STEPS

1. **enable**
2. **xconnect backup force-switchover interface {interface-info | peer ip-address vcid}**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                | Purpose                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>xconnect backup force-switchover {interface interface-info   peer ip-address vcid}</b><br><br><b>Example:</b><br>Router# xconnect backup force-switchover peer 10.10.10.1 123 | Specifies that the router should switch to the backup or to the primary pseudowire.                                 |

## Verifying the L2VPN Pseudowire Redundancy Configuration

Use the following commands to verify that the L2VPN Pseudowire Redundancy feature is correctly configured.

### SUMMARY STEPS

1. **show mpls l2transport vc**
2. **show xconnect all**
3. **xconnect logging redundancy**

### DETAILED STEPS

#### Step 1 show mpls l2transport vc

In this example, the primary attachment circuit is up. The backup attachment circuit is available, but not currently selected. The **show** output displays as follows:

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit | Dest address | VC ID | Status |
|------------|---------------|--------------|-------|--------|
| Eth0/0.1   | Eth VLAN 101  | 10.0.0.2     | 101   | UP     |

```
Local interface: Et0/0.1 up, line protocol up, Eth VLAN 101 up
  Destination address 10.0.0.2 VC ID: 101, VC status UP
  .
  .
  .
Local interface: Et0/0.1 down, line protocol down, Eth VLAN 101 down
  Destination address 10.0.0.3 VC ID: 201, VC status down
  .
  .
  .
```

## Step 2 show xconnect all

In this example, the topology is Attachment Circuit 1 to Pseudowire 1 with a Pseudowire 2 as a backup:

```
Router# show xconnect all
```

```

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
-----+-----+-----+-----+
UP pri ac Et0/0(Ethernet) UP mpls 10.55.55.2:1000 UP
IA sec ac Et0/0(Ethernet) UP mpls 10.55.55.3:1001 DN

```

In this example, the topology is Attachment Circuit 1 to Attachment Circuit 2 with a Pseudowire backup for Attachment Circuit 2:

```
Router# show xconnect all
```

```

Legend: XC ST=Xconnect State, S1=Segment1 State, S2=Segment2 State
UP=Up, DN=Down, AD=Admin Down, IA=Inactive, NH=No Hardware
XC ST Segment 1 S1 Segment 2 S2
-----+-----+-----+-----+
UP pri ac Se6/0:150(FR DLCI) UP ac Se8/0:150(FR DLCI) UP
IA sec ac Se6/0:150(FR DLCI) UP mpls 10.55.55.3:7151 DN

```

### Step 3 xconnect logging redundancy

In addition to the **show mpls l2transport vc** command and the **show xconnect** command, you can use the **xconnect logging redundancy** command to track the status of the xconnect redundancy group:

```
Router(config)# xconnect logging redundancy
```

When this command is configured, the following messages will be generated during switchover events:

Activating the primary member:

```
00:01:07: %XCONNECT-5-REDUNDANCY: Activating primary member 10.55.55.2:1000
```

Activating the backup member:

```
00:01:05: %XCONNECT-5-REDUNDANCY: Activating secondary member 10.55.55.3:1001
```

# Configuration Examples for L2VPN Pseudowire Redundancy

The following sections show the L2VPN Pseudowire Redundancy feature examples. These configuration examples show how the L2VPN Pseudowire Redundancy feature can be configured with the AToM (like-to-like), L2VPN Interworking, and Layer 2 Local Switching features.

- [L2VPN Pseudowire Redundancy and AToM \(Like to Like\): Examples, page 10](#)
- [L2VPN Pseudowire Redundancy and L2VPN Interworking: Examples, page 10](#)
- [L2VPN Pseudowire Redundancy with Layer 2 Local Switching: Examples, page 11](#)

Each of the configuration examples refers to one of the following pseudowire classes:

- AToM (like-to-like) pseudowire class:

```
pseudowire-class mpls
encapsulation mpls
```

- L2VPN IP interworking:

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

## L2VPN Pseudowire Redundancy and AToM (Like to Like): Examples

The following example shows a High-Level Data Link Control (HDLC) attachment circuit xconnect with a backup pseudowire:

```
interface Serial4/0
xconnect 10.55.55.2 4000 pw-class mpls
backup peer 10.55.55.3 4001 pw-class mpls
```

The following example shows a Frame Relay attachment circuit xconnect with a backup pseudowire:

```
connect fr-fr-pw Serial6/0 225 12transport
xconnect 10.55.55.2 5225 pw-class mpls
backup peer 10.55.55.3 5226 pw-class mpls
```

## L2VPN Pseudowire Redundancy and L2VPN Interworking: Examples

The following example shows an Ethernet attachment circuit xconnect with L2VPN IP interworking and a backup pseudowire:

```
interface Ethernet0/0
xconnect 10.55.55.2 1000 pw-class mpls-ip
backup peer 10.55.55.3 1001 pw-class mpls-ip
```

The following example shows an Ethernet VLAN attachment circuit xconnect with L2VPN IP interworking and a backup pseudowire:

```
interface Ethernet1/0.1
encapsulation dot1Q 200
no ip directed-broadcast
xconnect 10.55.55.2 5200 pw-class mpls-ip
backup peer 10.55.55.3 5201 pw-class mpls-ip
```

The following example shows a Frame Relay attachment circuit xconnect with L2VPN IP interworking and a backup pseudowire:



```
connect fr-ppp-pw Serial6/0 250 l2transport
xconnect 10.55.55.2 8250 pw-class mpls-ip
backup peer 10.55.55.3 8251 pw-class mpls-ip
```

The following example shows a PPP attachment circuit xconnect with L2VPN IP interworking and a backup pseudowire:

```
interface Serial7/0
encapsulation ppp
xconnect 10.55.55.2 2175 pw-class mpls-ip
backup peer 10.55.55.3 2176 pw-class mpls-ip
```

## L2VPN Pseudowire Redundancy with Layer 2 Local Switching: Examples

The following example shows an Ethernet VLAN-VLAN local switching xconnect with a pseudowire backup for Ethernet segment E2/0.2. If the subinterface associated with E2/0.2 goes down, the backup pseudowire is activated.

```
connect vlan-vlan Ethernet1/0.2 Ethernet2/0.2
backup peer 10.55.55.3 1101 pw-class mpls
```

The following example shows a Frame Relay-to-Frame Relay local switching connect with a pseudowire backup for Frame Relay segment S8/0 150. If data-link connection identifier (DLCI) 150 on S8/0 goes down, the backup pseudowire is activated.

```
connect fr-fr-ls Serial6/0 150 Serial8/0 150
backup peer 10.55.55.3 7151 pw-class mpls
```

# Additional References

The following sections provide references related to the L2VPN Pseudowire Redundancy feature.

## Related Documents

| Related Topic              | Document Title                                                                                      |
|----------------------------|-----------------------------------------------------------------------------------------------------|
| Any Transport over MPLS    | <a href="#"><i>Any Transport over MPLS</i></a>                                                      |
| High Availability for AToM | <a href="#"><i>AToM Graceful Restart</i></a>                                                        |
| L2VPN Interworking         | <a href="#"><i>L2VPN Interworking</i></a>                                                           |
| Layer 2 local switching    | <a href="#"><i>Layer 2 Local Switching</i></a>                                                      |
| PWE3 MIB                   | <a href="#"><i>Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services</i></a> |
| Packet sequencing          | <a href="#"><i>Any Transport over MPLS (AToM) Sequencing Support</i></a>                            |

## Standards

| Standards | Title |
|-----------|-------|
| None      | —     |

## MIBs

| MIBs | MIBs Link                                                                                                                                                                                                              |
|------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **backup delay (L2VPN local switching)**
- **backup peer**
- **show xconnect**
- **xconnect backup force-switchover**
- **xconnect logging redundancy**

## Feature Information for L2VPN Pseudowire Redundancy

[Table 1](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 1**      **Feature Information for L2VPN Pseudowire Redundancy**

| Feature Name                           | Releases                                                                                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2VPN Pseudowire Redundancy            | 12.0(31)S<br>12.2(28)SB<br>12.4(11)T<br>12.2(33)SRB<br>12.2(22)SXI<br>Cisco IOS XE<br>Release 2.3 | <p>This feature enables you to set up your network to detect a failure in the network and reroute the Layer 2 service to another endpoint that can continue to provide service.</p> <p>In Cisco IOS Release 12.0(31)S, the L2VPN Pseudowire Redundancy feature was introduced for Any Transport over MPLS (AToM) on the Cisco 12000 series routers.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.4(11)T.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXI.</p> <p>In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Introduction to L2VPN Pseudowire Redundancy, page 3</a></li> <li>• <a href="#">Configuring the Pseudowire, page 5</a></li> <li>• <a href="#">Configuring L2VPN Pseudowire Redundancy, page 6</a></li> <li>• <a href="#">Forcing a Manual Switchover to the Backup Pseudowire VC, page 8</a></li> <li>• <a href="#">Verifying the L2VPN Pseudowire Redundancy Configuration, page 8</a></li> </ul> <p>The following commands were introduced or modified: <b>backup delay</b> (L2VPN local switching), <b>backup peer</b>, <b>show xconnect</b>, <b>xconnect backup force-switchover</b>, <b>xconnect logging redundancy</b>.</p> |
| L2VPN Pseudowire Redundancy for L2TPv3 | 12.2(33)SRE                                                                                       | <p>This feature provides L2VPN pseudowire redundancy for L2TPv3 xconnect configurations.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was implemented on the Cisco 7600 series routers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLynx, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream,

Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.



# L2VPN Pseudowire Switching

---

**First Published: April 20, 2005**

**Last Updated: November 20, 2009**

This feature module explains how to configure L2VPN Pseudowire Switching, which extends Layer 2 Virtual Private Network (L2VPN) pseudowires across an interautonomous system (inter-AS) boundary or across two separate Multiprotocol Label Switching (MPLS) networks. The feature supports ATM and time-division multiplexing (TDM) attachment circuits (ACs) and Ethernet ACs.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for L2VPN Pseudowire Switching”](#) section on page 15.

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

## Contents

- [Prerequisites for L2VPN Pseudowire Switching, page 2](#)
- [Restrictions for L2VPN Pseudowire Switching, page 2](#)
- [Information About L2VPN Pseudowire Switching, page 2](#)
- [How to Configure L2VPN Pseudowire Switching, page 4](#)
- [Configuration Examples for L2VPN Pseudowire Switching, page 7](#)
- [Additional References, page 12](#)
- [Feature Information for L2VPN Pseudowire Switching, page 15](#)



---

**Americas Headquarters:**

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

## Prerequisites for L2VPN Pseudowire Switching

For the Cisco 12000 series routers, the L2VPN Pseudowire Switching feature for Any Transport over MPLS (AToM) is supported on the following engines:

- E2
- E3
- E4+
- E5
- E6

For engines that do not support this feature, the packets are sent to the software and forwarded through the slow path.

**Note**

---

Engines E1 and E4 do not support L2VPN Pseudowire Switching, even in the slow path.

---

## Restrictions for L2VPN Pseudowire Switching

- L2VPN Pseudowire Switching is supported with AToM.
- Only static, on-box provisioning is supported.
- Sequencing numbers in AToM packets are not processed by L2VPN Pseudowire Switching. The feature blindly passes the sequencing data through the xconnect packet paths, a process that is called transparent sequencing. The endpoint provider-edge (PE) to customer-edge (CE) connections enforce the sequencing.
- You can ping the adjacent next-hop PE router. End-to-end label switched path (LSP) pings are not supported.
- Do not configure IP or Ethernet interworking on a router where L2VPN Pseudowire Switching is enabled. Instead, configure interworking on the routers at the edge PEs of the network.
- The control word negotiation results must match. If either segment does not negotiate the control word, the control word is disabled for both segments.
- AToM Graceful Restart is negotiated independently on each pseudowire segment. If there is a transient loss of the label distribution protocol (LDP) session between two AToM PE routers, packets continue to flow.
- Per-pseudowire quality of service (QoS) is not supported. Traffic engineering (TE) tunnel selection is supported.
- Attachment circuit interworking is not supported.

## Information About L2VPN Pseudowire Switching

To configure the L2VPN Pseudowire Switching feature, you should understand the following concepts:

- [How L2VPN Pseudowire Switching Works, page 3](#)
- [How Packets Are Manipulated at the L2VPN Pseudowire Switching Aggregation Point, page 3](#)



## How L2VPN Pseudowire Switching Works

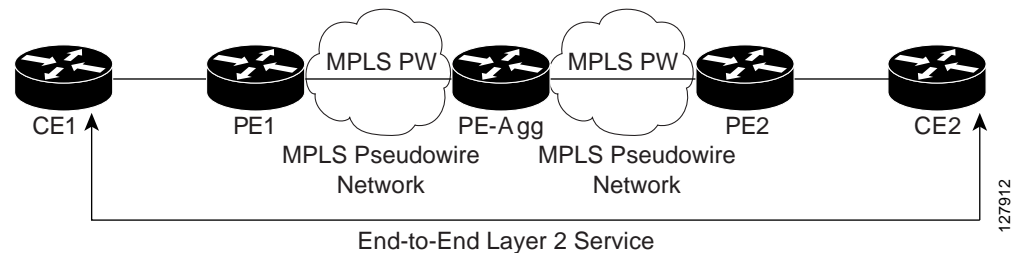
L2VPN Pseudowire Switching allows the user to extend L2VPN pseudowires across two separate MPLS networks or across an inter-AS boundary, as shown in [Figure 1](#) and [Figure 2](#).

L2VPN Pseudowire Switching connects two or more contiguous pseudowire segments to form an end-to-end multihop pseudowire. This end-to-end pseudowire functions as a single point-to-point pseudowire.

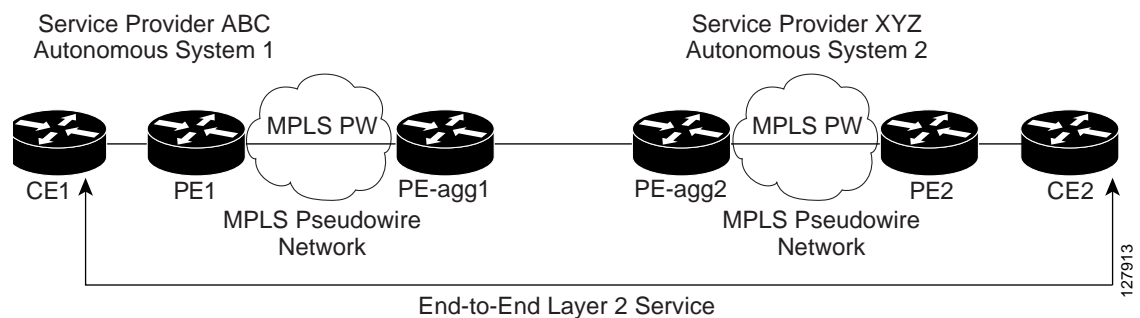
As shown in [Figure 2](#), L2VPN Pseudowire Switching enables you to keep the IP addresses of the edge PE routers private across inter-AS boundaries. You can use the IP address of the Autonomous System Boundary Routers (ASBRs) and treat them as pseudowire aggregation (PE-agg) routers. The ASBRs join the pseudowires of the two domains.

L2VPN Pseudowire Switching also enables you to keep different administrative or provisioning domains to manage the end-to-end service. At the boundaries of these networks, PE-agg routers delineate the management responsibilities.

**Figure 1** L2VPN Pseudowire Switching in an Intra-AS Topology



**Figure 2** L2VPN Pseudowire Switching in an Inter-AS Topology



## How Packets Are Manipulated at the L2VPN Pseudowire Switching Aggregation Point

Switching AToM packets between two AToM pseudowires is the same as switching any MPLS packet. The MPLS switching data path switches AToM packets between two AToM pseudowires. The following list explains exceptions:

- The outgoing virtual circuit (VC) label replaces the incoming VC label in the packet. New Internal Gateway Protocol (IGP) labels and Layer 2 encapsulation are added.

- The incoming VC label time-to-live (TTL) field is decremented by one and copied to the outgoing VC label TTL field.
- The incoming VC label EXP value is copied to the outgoing VC label EXP field.
- The outgoing VC label “Bottom of Stack” S bit in the outgoing VC label is set to 1.
- AToM control word processing is not performed at the L2VPN Pseudowire Switching aggregation point. Sequence numbers are not validated. Use the Router Alert label for LSP Ping; do not require control word inspection to determine an LSP Ping packet.

## How to Configure L2VPN Pseudowire Switching

Use the following procedure to configure L2VPN Pseudowire Switching on each of the PE-aggr routers.

### Prerequisites

- This procedure assumes that you have configured basic AToM L2VPNs. This procedure does not explain how to configure basic AToM L2VPNs that transport Layer 2 packets over an MPLS backbone. For information on the basic configuration, see [Any Transport over MPLS](#).
- For interautonomous configurations, ASBRs require a labeled interface.

### Restrictions

In this configuration, you are limited to two **neighbor** commands after entering the **l2 vfi** command.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 vfi *name* point-to-point**
4. **neighbor *ip-address* *vcid* [encapsulation *mpls* | pw-class *pw-class-name*]**
5. **exit**
6. **exit**
7. **show mpls l2transport vc [*vcid* [*vc-id* | *vc-id-min* *vc-id-max*]] [**interface** *name* [*local-circuit-id*]] [**destination** *ip-address* | *name*] [**detail**]**
8. **show vfi [*vfi-name*]**

## 9. ping [protocol] [tag] {host-name | system-address}

### DETAILED STEPS

|         | Command or Action                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                 |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1  | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                        |
| Step 2  | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                               | Enters global configuration mode.                                                                                                                                                                                                                                                                                       |
| Step 3  | <b>l2 vfi name point-to-point</b><br><br><b>Example:</b><br>Router(config)# l2 vfi atomtunnel point-to-point                                                                                                 | Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.                                                                                                                                                                                                                  |
| Step 4  | <b>neighbor ip-address vcid [encapsulation mpls   pw-class pw-class-name]</b><br><br><b>Example:</b><br>Router(config-vfi)# neighbor 10.0.0.1 100 pw-class mpls                                              | Configures an emulated VC. <ul style="list-style-type: none"> <li>Specify the IP address and the VC ID of the remote router.</li> <li>Also specify the pseudowire class to use for the emulated VC.</li> </ul> <b>Note</b> Only two <b>neighbor</b> commands are allowed for each <b>l2 vfi point-to-point</b> command. |
| Step 5  | <b>exit</b><br><br><b>Example:</b><br>Router(config-vfi)# exit                                                                                                                                               | Exits VFI configuration mode.                                                                                                                                                                                                                                                                                           |
| Step 6  | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                   | Exits global configuration mode.                                                                                                                                                                                                                                                                                        |
| Step 7s | <b>show mpls l2transport vc [vcid [vc-id   vc-id-min vc-id-max]] [interface name [local-circuit-id]] [destination ip-address   name] [detail]</b><br><br><b>Example:</b><br>Router# show mpls l2transport vc | Verifies that the L2VPN Pseudowire Switching session has been established.                                                                                                                                                                                                                                              |

|        | Command or Action                                                                                                            | Purpose                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Step 8 | <code>show vfi [vfi-name]</code><br><br><b>Example:</b><br>Router# <code>show vfi atomtunnel</code>                          | Verifies that a point-to-point VFI has been established.           |
| Step 9 | <code>ping [protocol] [tag] {host-name   system-address}</code><br><br><b>Example:</b><br>Router# <code>ping 10.1.1.1</code> | When issued from the CE routers, verifies end-to-end connectivity. |

## Examples

The following example displays output from the **show mpls l2transport vc** command:

```
Router# show mpls l2transport vc
```

| Local intf | Local circuit | Dest address | VC ID | Status |
|------------|---------------|--------------|-------|--------|
| MPLS PW    | 10.0.1.1:100  | 10.0.1.1     | 100   | UP     |
| MPLS PW    | 10.0.1.1:100  | 10.0.1.1     | 100   | UP     |

The following example displays output from the **show vfi** command:

```
Router# show vfi
```

```
VFI name: test, type: point-to-point
Neighbors connected via pseudowires:
  Router ID      Pseudowire ID
  10.0.1.1       100
  10.0.1.1       100
```

# Configuration Examples for L2VPN Pseudowire Switching

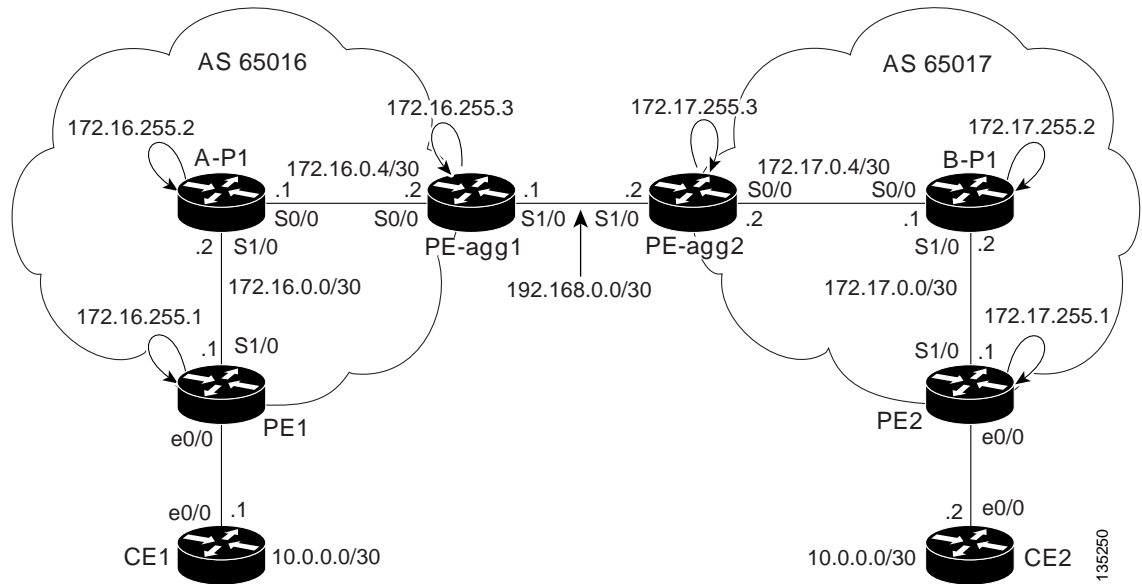
This section provides the following configuration example:

- [L2VPN Pseudowire Switching in an Inter-AS Configuration: Example, page 7](#)

## L2VPN Pseudowire Switching in an Inter-AS Configuration: Example

Two separate autonomous systems are able to pass L2VPN packets, because the two PE-aggr routers have been configured with L2VPN Pseudowire Switching. This example configuration is shown in [Figure 3](#).

**Figure 3** L2VPN Pseudowire Switching in an Interautonomous System



**PE-agg-1**

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname [pe-agg1]
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$Q0Bb$32sIU82pHRgyddWaeB4zs/
!
ip subnet-zero
ip cef
no ip domain-lookup
mpls label protocol ldp
pseudowire-class SW-PW
    encapsulation mpls
!
12 vfi PW-SWITCH-1 point-to-point
    neighbor 172.17.255.3 100 pw-class SW-PW
    neighbor 172.16.255.1 16 pw-class SW-PW
!
interface Loopback0
    ip address 172.16.255.3 255.255.255.255
    no ip directed-broadcast
!
interface Serial0/0
    ip address 172.16.0.6 255.255.255.252
    no ip directed-broadcast
    mpls ip
!
interface Serial1/0
    ip address 192.168.0.1 255.255.255.252
    no ip directed-broadcast
    mpls bgp forwarding
!
router ospf 16
    log-adjacency-changes
    network 172.16.0.0 0.0.255.255 area 0
!
router bgp 65016
    no synchronization
    bgp log-neighbor-changes
    network 172.16.255.3 mask 255.255.255.255
    neighbor 192.168.0.2 remote-as 65017
    neighbor 192.168.0.2 send-label
    no auto-summary
!
ip classless
control-plane
!
line con 0
    exec-timeout 0 0
line aux 0
line vty 0 4
    login
!
no cns aaa enable
end

```

**PE-agg-2**

```

version 12.0
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname [pe-agg2]
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$32jd$zQRfxXzjstr41lV9DcWf7/
!
ip subnet-zero
ip cef
no ip domain-lookup
mpls label protocol ldp
pseudowire-class SW-PW
    encapsulation mpls
!
12 vfi PW-SWITCH-1 point-to-point
    neighbor 172.16.255.3 100 pw-class SW-PW
    neighbor 172.17.255.1 17 pw-class SW-PW
!
interface Loopback0
    ip address 172.17.255.3 255.255.255.255
    no ip directed-broadcast
!
interface Serial0/0
    ip address 172.17.0.6 255.255.255.252
    no ip directed-broadcast
    mpls ip
!
interface Serial1/0
    ip address 192.168.0.2 255.255.255.252
    no ip directed-broadcast
    mpls bgp forwarding
!
router ospf 17
    log-adjacency-changes
    network 172.17.0.0 0.0.255.255 area 0
!
router bgp 65017
    no synchronization
    bgp log-neighbor-changes
    network 172.17.255.3 mask 255.255.255.255
    neighbor 192.168.0.1 remote-as 65016
    neighbor 192.168.0.1 send-label
    no auto-summary
!
ip classless
control-plane
!
line con 0
    exec-timeout 0 0
line aux 0
line vty 0 4
    login
!
no cns aaa enable
end

```

| A-P1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | B-P1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [a-p1] ! boot-start-marker boot-end-marker ! enable secret 5 \$l\$eiUn\$rTMnZiYnJxtMTpO0NKpQQ/ ! ip subnet-zero ip cef no ip domain-lookup mpls label protocol ldp ! interface Loopback0  ip address 172.16.255.2 255.255.255.255  no ip directed-broadcast ! interface Serial0/0  ip address 172.16.0.5 255.255.255.252  no ip directed-broadcast  mpls ip ! interface Serial1/0  ip address 172.16.0.2 255.255.255.252  no ip directed-broadcast  mpls ip ! router ospf 16  log-adjacency-changes  network 172.16.0.0 0.0.255.255 area 0 ! ip classless ! control-plane ! line con 0  exec-timeout 0 0 line aux 0 line vty 0 4  login ! no cns aaa enable end </pre> | <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [b-p1] ! boot-start-marker boot-end-marker ! enable secret 5 \$l\$svU/\$2JmJZ/5gxlW4nVXVniIJel ! ip subnet-zero ip cef no ip domain-lookup mpls label protocol ldp ! interface Loopback0  ip address 172.17.255.2 255.255.255.255  no ip directed-broadcast ! interface Serial0/0  ip address 172.17.0.5 255.255.255.252  no ip directed-broadcast  mpls ip ! interface Serial1/0  ip address 172.17.0.2 255.255.255.252  no ip directed-broadcast  mpls ip ! router ospf 17  log-adjacency-changes  network 172.17.0.0 0.0.255.255 area 0 ! ip classless ! control-plane ! line con 0  exec-timeout 0 0 line aux 0 line vty 0 4  login ! no cns aaa enable end </pre> |



| PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [pe1] ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$9z8F\$2A1/YLc6NB6d.WLQXF0Bz1 ! ip subnet-zero ip cef no ip domain-lookup mpls label protocol ldp pseudowire-class ETH-PW encapsulation mpls ! interface Loopback0  ip address 172.16.255.1 255.255.255.255  no ip directed-broadcast ! interface Ethernet0/0  no ip address  no ip directed-broadcast  no cdp enable  xconnect 172.16.255.3 16 pw-class ETH-PW ! interface Serial1/0  ip address 172.16.0.1 255.255.255.252  no ip directed-broadcast  mpls ip ! router ospf 16  log-adjacency-changes  network 172.16.0.0 0.0.255.255 area 0 ! ip classless ! control-plane ! line con 0  exec-timeout 0 0 line aux 0 line vty 0 4  login ! no cns aaa enable end </pre> | <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [pe2] ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$rT.V\$8Z6Dy/r8/eaRdx2TR/O5r/ ! ip subnet-zero ip cef no ip domain-lookup mpls label protocol ldp pseudowire-class ETH-PW encapsulation mpls ! interface Loopback0  ip address 172.17.255.1 255.255.255.255  no ip directed-broadcast ! interface Ethernet0/0  no ip address  no ip directed-broadcast  no cdp enable  xconnect 172.17.255.3 17 pw-class ETH-PW ! interface Serial1/0  ip address 172.17.0.1 255.255.255.252  no ip directed-broadcast  mpls ip ! router ospf 17  log-adjacency-changes  network 172.17.0.0 0.0.255.255 area 0 ! ip classless ! control-plane ! line con 0  exec-timeout 0 0 line aux 0 line vty 0 4  login ! no cns aaa enable end </pre> |

| CE1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [ce1] ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$o9N6\$LSrxHufTn0vjCY0nW8hQX. ! ip subnet-zero ip cef no ip domain-lookup ! interface Ethernet0/0  ip address 10.0.0.1 255.255.255.252  no ip directed-broadcast ! ip classless ! control-plane ! line con 0   exec-timeout 0 0 line aux 0 line vty 0 4   login ! no cns aaa enable end </pre> | <pre> version 12.0 service timestamps debug uptime service timestamps log uptime service password-encryption ! hostname [ce2] ! boot-start-marker boot-end-marker ! enable secret 5 \$1\$YHo6\$LQ4z5PdrF5B9dnL75Xvvm1 ! ip subnet-zero ip cef no ip domain-lookup ! interface Ethernet0/0  ip address 10.0.0.2 255.255.255.252  no ip directed-broadcast ! ip classless ! control-plane ! line con 0   exec-timeout 0 0 line aux 0 line vty 0 4   login ! no cns aaa enable end </pre> |

## Additional References

The following sections provide references related to L2VPN Pseudowire Switching.

## Related Documents

| Related Topic              | Document Title                                                                               |
|----------------------------|----------------------------------------------------------------------------------------------|
| Any Transport over MPLS    | <a href="#">Any Transport over MPLS</a>                                                      |
| Pseudowire redundancy      | <a href="#">L2VPN Pseudowire Redundancy</a>                                                  |
| High availability for AToM | <a href="#">AToM Graceful Restart</a>                                                        |
| L2VPN interworking         | <a href="#">L2VPN Interworking</a>                                                           |
| Layer 2 local switching    | <a href="#">Layer 2 Local Switching</a>                                                      |
| PWE3 MIB                   | <a href="#">Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services</a> |
| Packet sequencing          | <a href="#">Any Transport over MPLS (AToM) Sequencing Support</a>                            |

## Standards

| Standard                                | Title                                                      |
|-----------------------------------------|------------------------------------------------------------|
| draft-ietf-pwe3-control-protocol-14.txt | <a href="#">Pseudowire Setup and Maintenance using LDP</a> |
| draft-martini-pwe3-pw-switching-01.txt  | <a href="#">Pseudo Wire Switching</a>                      |

## MIBs

| MIB                                                                                                                                                               | MIBs Link                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>CISCO-IETF-PW-MIB</li> <li>CISCO-IETF-PW-MPLS-MIB</li> <li>CISCO-IETF-PW-ENET-MIB</li> <li>CISCO-IETF-PW-FR-MIB</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for L2VPN Pseudowire Switching

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(28)SB or 12.2(33)SRB or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for L2VPN Pseudowire Switching

| Feature Name               | Releases                                                              | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2VPN Pseudowire Switching | 12.0(31)S<br>12.2(28)SB<br>12.2(33)SRB<br>12.2(33)SRD2<br>12.2(33)SRE | This feature configures L2VPN Pseudowire Switching, which extends L2VPN pseudowires across an interautonomous system (inter-AS) boundary or across two separate MPLS networks.<br><br>In Cisco IOS Release 12.2(28)SB, support was added for the Cisco 7200 and 7301 series routers.<br><br>In 12.2(33)SRD2, support was added for ATM and TDM ACs.<br><br>The following commands were introduced or modified: <b>12 vfi point-to-point, neighbor</b> (L2VPN Pseudowire Switching), <b>show vfi</b> . |

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

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

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.



# VPLS Autodiscovery: BGP Based

---

**First Published: February 19, 2007**

**Last Updated: November 20, 2009**

VPLS Autodiscovery enables each Virtual Private LAN Service (VPLS) provider edge (PE) router to discover which other PE routers are part of the same VPLS domain. VPLS Autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain. You no longer need to manually configure the VPLS and maintain the configuration when a PE router is added or deleted. VPLS Autodiscovery uses the Border Gateway Protocol (BGP) to discover the VPLS members and to set up and tear down pseudowires in the VPLS.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for VPLS Autodiscovery: BGP Based”](#) section on page 16.

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

## Contents

- [Prerequisites for VPLS Autodiscovery: BGP Based, page 2](#)
- [Restrictions for VPLS Autodiscovery: BGP Based, page 2](#)
- [Information About VPLS Autodiscovery: BGP Based, page 3](#)
- [How to Configure VPLS Autodiscovery: BGP Based, page 5](#)
- [Configuration Examples for VPLS Autodiscovery: BGP Based, page 11](#)
- [Additional References, page 14](#)
- [Feature Information for VPLS Autodiscovery: BGP Based, page 16](#)



---

**Americas Headquarters:**

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for VPLS Autodiscovery: BGP Based

Before configuring VPLS Autodiscovery, if you are using a Cisco 7600 series router, perform the Cisco 7600 router-specific tasks listed in the section called “Virtual Private LAN Services on the Optical Service Modules” in the *Cisco 7600 Series Router IOS Software Configuration Guide, 12.2SR*.

## Restrictions for VPLS Autodiscovery: BGP Based

- VPLS Autodiscovery supports only IPv4 addresses.
- VPLS Autodiscovery uses Forwarding Equivalence Class (FEC) 129 to convey endpoint information. Manually configured pseudowires use FEC 128.
- VPLS Autodiscovery is not supported with Layer 2 Tunnel Protocol Version 3 (L2TPv3).
- VPLS Autodiscovery is not supported with interautonomous system configurations.
- You can configure both autodiscovered and manually configured pseudowires in a single virtual forwarding instance (VFI). However, the pseudowires cannot go to the same peer PE router.
- If you manually configure a neighbor using the **neighbor (VPLS)** command after you have enabled VPLS Autodiscovery and both peers are in autodiscovery mode, manually configure the route target (RT) values to prevent each peer from receiving discovery data for that VPLS.
- If you manually configure multiple pseudowires and target different IP addresses on the same PE router for each pseudowire, do not use the same virtual circuit identifier (VC ID) to identify the pseudowires terminated at the same PE router.
- You cannot configure a pseudowire by manually configuring a neighbor on one PE router and using autodiscovery on the other PE router to configure the same pseudowire in the other direction.
- Tunnel selection is not supported with autodiscovered neighbors.
- You can have up to 16 route targets only per VFI.
- The same RT is not allowed in multiple VFIs in the same PE router.
- The BGP autodiscovery process does not support dynamic hierarchical VPLS. User-facing PE (U-PE) routers cannot discover the network-facing PE (N-PE) routers, and N-PE routers cannot discover U-PE routers.
- Pseudowires for autodiscovered neighbors are provisioned with split horizon enabled. Therefore, manually configure the pseudowires for hierarchical VPLS. Make sure the U-PE routers do not participate in BGP autodiscovery for those pseudowires.
- Do not disable split horizon on autodiscovered neighbors. Split horizon is required with VPLS Autodiscovery.
- The provisioned peer address must be a /32 address bound to the peer's Label Distribution Protocol (LDP) router ID.
- The peer PE router must be able to access the IP address that is used as the local LDP router ID. Even though the IP address need not be used in the **xconnect** command on the peer PE router, that IP address must be reachable.
- VPLS Autodiscovery is supported on the Cisco 7600 router hardware. For details on supported shared port adapters and line cards, see the following documents:
  - *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*
  - *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*



# Information About VPLS Autodiscovery: BGP Based

To understand VPLS Autodiscovery, you should understand the following concepts:

- [How the VPLS Feature Works, page 3](#)
- [How the VPLS Autodiscovery: BGP Based Feature Works, page 3](#)
- [How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS, page 3](#)
- [Show Commands Affected by VPLS Autodiscovery: BGP Based, page 4](#)
- [BGP VPLS Autodiscovery Support on a Route Reflector, page 4](#)

## How the VPLS Feature Works

VPLS allows Multiprotocol Label Switching (MPLS) networks to provide multipoint Ethernet LAN services, also known as Transparent LAN Services (TLS). All customer sites in a VPLS appear to be on the same LAN, even though those sites might be in different geographic locations.

## How the VPLS Autodiscovery: BGP Based Feature Works

VPLS Autodiscovery enables each VPLS PE router to discover the other PE routers that are part of the same VPLS domain. VPLS Autodiscovery also tracks when PE routers are added to or removed from the VPLS domain. The autodiscovery and signaling functions use BGP to find and track the PE routers.

BGP uses the L2VPN Routing Information Base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 VFI is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make decisions on the best path. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the configuration of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network. For more information about BGP and the L2VPN address family in relation to VPLS Autodiscovery, see the following documents:

- The section called “L2VPN Address Family” in the [Cisco BGP Overview](#).
- The document called [BGP Support for the L2VPN Address Family](#)

## How Enabling VPLS Autodiscovery Differs from Manually Configuring VPLS

With VPLS Autodiscovery, you no longer need to manually set up the VPLS. The commands you use to set up VPLS Autodiscovery are similar to those you use to manually configure a VPLS, as shown in [Table 1](#). VPLS Autodiscovery uses **neighbor** commands in L2VPN address family mode to distribute endpoint information to configure a pseudowire.

**Table 1** VPLS Autodiscovery Configuration versus Manual VPLS Configuration

| Manual Configuration of VPLS                                                                                                 | VPLS Autodiscovery: BGP Based                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>l2 vfi vpls1 manual vpn id 100 neighbor 10.10.10.1 encapsulation mpls neighbor 10.10.10.0 encapsulation mpls exit</pre> | <pre>l2 vfi vpls1 autodiscovery vpn id 100 exit  router bgp 1 no bgp default ipv4-unicast bgp log-neighbor-changes bgp update-delay 1 neighbor 10.1.1.2 remote-as 1 neighbor 10.1.1.2 update-source Loopback1 . . . address-family l2vpn vpls neighbor 10.1.1.2 activate neighbor 10.1.1.2 send-community extended exit-address-family</pre> |

When you configure VPLS Autodiscovery, you enter the **l2vfi autodiscovery** command. This command allows the VFI to learn and advertise the pseudowire endpoints. As a result, you no longer need to enter the **neighbor (VPLS)** command in L2 VFI configuration mode.

However, the **neighbor (VPLS)** command is still supported with VPLS Autodiscovery in L2 VFI command mode. You can use the **neighbor (VPLS)** command to allow PE routers that do not participate in the autodiscovery process to join the VPLS. You can also use the **neighbor (VPLS)** command with PE routers that have been configured using the Tunnel Selection feature. You can also use the **neighbor (VPLS)** command in hierarchical VPLS configurations that have U-PE routers that do not participate in the autodiscovery process and have split-horizon forwarding disabled.

## Show Commands Affected by VPLS Autodiscovery: BGP Based

VPLS Autodiscovery changes the following show commands:

- The **show mpls l2transport vc** command with the **detail** keyword has been updated to include FEC 129 signaling information for the autodiscovered VPLS pseudowires.
- The **show vfi** command now displays information related to autodiscovered VFIs. The new information includes the VPLS ID, the route distinguisher (RD), the RT, and the router IDs of the discovered peers.
- The **show xconnect** command has been updated with the **rib** keyword to provide RIB information about the pseudowires.

## BGP VPLS Autodiscovery Support on a Route Reflector

VPLS Autodiscovery is normally run on PE routers to support endpoint discovery and the setup of pseudowires between the PEs (typically a full mesh). VPLS does not normally run on a BGP route reflector. In Cisco IOS Release 12.2(33)SRE, VPLS Autodiscovery support was added to route reflectors. The BGP route reflector can be used to reflect the BGP VPLS prefixes without having VPLS explicitly configured on the route reflector.

The route reflector does not participate in the autodiscovery, meaning that no pseudowires are set up between the route reflector and the PEs. The route reflector reflects the VPLS prefixes to other PEs, so that the PEs do not need to have a full mesh of BGP sessions. The network administrator configures only the BGP VPLS address family on the route reflector. For an example configuration of VPLS autodiscovery support on a route reflector, see the [“BGP VPLS Autodiscovery Support on Route Reflector: Example” section on page 13](#).

## How to Configure VPLS Autodiscovery: BGP Based

To configure VPLS Autodiscovery, perform the following tasks:

- [Enabling VPLS Autodiscovery: BGP Based, page 5](#) (required)
- [Configuring BGP to Enable VPLS Autodiscovery, page 6](#) (required)
- [Customizing the VPLS Autodiscovery Settings, page 9](#) (optional)

### Enabling VPLS Autodiscovery: BGP Based

Perform the following task to enable each VPLS PE router to discover the other PE routers that are part of the same VPLS domain.

#### Prerequisites

Before configuring VPLS Autodiscovery, perform the Cisco 7600 router-specific tasks listed in the “Virtual Private LAN Services on the Optical Services Modules” chapter in the [Cisco 7600 Series Router Cisco IOS Software Configuration Guide](#), Release 12.2SR.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 vfi vfi-name autodiscovery**
4. **vpn id vpn-id**
5. **exit**

#### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                          |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                  |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                  |

|        | Command or Action                                                                                         | Purpose                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Step 3 | <b>l2 vfi vfi-name autodiscovery</b><br><br><b>Example:</b><br>Router(config)# l2 vfi vpls1 autodiscovery | Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.                       |
| Step 4 | <b>vpn id vpn-id</b><br><br><b>Example:</b><br>Router(config-vfi)# vpn id 10                              | Configures a VPN ID for the VPLS domain.                                                                |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vfi)# exit                                            | Exits L2 VFI configuration mode. Commands take effect after the router exits L2 VFI configuration mode. |

## Configuring BGP to Enable VPLS Autodiscovery

In Cisco IOS Release 12.2(33)SRB, the BGP L2VPN address family was introduced with a separate L2VPN RIB that contains endpoint provisioning information for VPLS Autodiscovery. BGP learns the endpoint provisioning information from the L2VPN database which is updated each time a Layer 2 virtual forwarding instance (VFI) is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to configure a pseudowire mesh to support aL2VPN-based services.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp autonomous-system-number**
4. **no bgp default ipv4-unicast**
5. **bgp log-neighbor-changes**
6. **neighbor {ip-address | peer-group-name} remote-as autonomous-system-number**
7. **neighbor {ip-address | peer-group-name} update-source interface**
8. Repeat Step 6 and Step 7 to configure other BGP neighbors.
9. **address-family l2vpn [vpls]**
10. **neighbor {ip-address | peer-group-name} activate**
11. **neighbor {ip-address | peer-group-name} send-community [both | standard | extended]**
12. Repeat Step 10 and Step 11 to activate other BGP neighbors under L2VPN address family.
13. **exit-address-family**
14. **exit**
15. **exit**
16. **show vfi**
17. **show ip bgp l2vpn vpls {all | rd vpn-rd}**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>router bgp <i>autonomous-system-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 65000                                                                                          | Enters router configuration mode for the specified routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast                                                                                       | Disables the IPv4 unicast address family for the BGP routing process. <p><b>Note</b> Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session configured with the <b>neighbor remote-as</b> router configuration command unless you configure the <b>no bgp default ipv4-unicast</b> router configuration command before configuring the <b>neighbor remote-as</b> command. Existing neighbor configurations are not affected.</p>                                                                                                                                                                       |
| Step 5 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                                             | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 6 | <b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>}</b><br><b>remote-as <i>autonomous-system-number</i></b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.1 remote-as 65000 | Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>If the <i>autonomous-system-number</i> argument matches the autonomous system number specified in the <b>router bgp</b> command, the neighbor is an internal neighbor.</li> <li>If the <i>autonomous-system-number</i> argument does not match the autonomous system number specified in the <b>router bgp</b> command, the neighbor is an external neighbor.</li> <li>In this example, the neighbor at 10.10.10.1 is an internal BGP neighbor.</li> </ul> |

|         | Command or Action                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                 |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>update-source</b> <i>interface-type interface-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.1<br>update-source loopback1                  | (Optional) Configures a router to select a specific source or interface to receive routing table updates. <ul style="list-style-type: none"> <li>This example uses a loopback interface. The advantage to this configuration is that the loopback interface is not affected by the effects of a flapping interface.</li> </ul>          |
| Step 8  | Repeat Step 6 and Step 7 to configure other BGP neighbors                                                                                                                                                                                      | —                                                                                                                                                                                                                                                                                                                                       |
| Step 9  | <b>address-family</b> l2vpn [ <b>vpls</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family l2vpn<br>vpls                                                                                                                      | Specifies the L2VPN address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The optional <b>vpls</b> keyword specifies that VPLS endpoint provisioning information is to be distributed to BGP peers.</li> <li>In this example, an L2VPN VPLS address family session is created.</li> </ul> |
| Step 10 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.10.10.1<br>activate                                                                          | Enables the neighbor to exchange information for the L2VPN VPLS address family with the local router.                                                                                                                                                                                                                                   |
| Step 11 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>send-community</b> { <b>both</b>   <b>standard</b>   <b>extended</b> }<br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.10.10.1<br>send-community extended | Specifies that a communities attribute should be sent to a BGP neighbor. <ul style="list-style-type: none"> <li>In this example, an extended communities attribute is sent to the neighbor at 10.10.10.1.</li> </ul>                                                                                                                    |
| Step 12 | Repeat Step 10 and Step 11 to activate other BGP neighbors under an L2VPN address family.                                                                                                                                                      | —                                                                                                                                                                                                                                                                                                                                       |
| Step 13 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                                                                             | Exits address family configuration mode and returns to router configuration mode.                                                                                                                                                                                                                                                       |
| Step 14 | <b>exit</b><br><br><b>Example:</b><br>Router(config-router)# exit                                                                                                                                                                              | Exits router configuration mode.                                                                                                                                                                                                                                                                                                        |
| Step 15 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit                                                                                                                                                                                     | Exits privileged EXEC mode.                                                                                                                                                                                                                                                                                                             |

|         | Command or Action                                                                                                 | Purpose                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Step 16 | <pre>show vfi</pre> <p><b>Example:</b><br/>Router# show vfi</p>                                                   | (Optional) Displays information about the configured VFI instances.       |
| Step 17 | <pre>show ip bgp l2vpn vpls {all   rd vpn-rd}</pre> <p><b>Example:</b><br/>Router# show ip bgp l2vpn vpls all</p> | (Optional) Displays information about the Layer2 VPN VPLS address family. |

## Customizing the VPLS Autodiscovery Settings

Several commands allow you to customize the VPLS environment. You can specify identifiers for the VPLS domain, the route distinguisher, the route target, and the PE router. Perform the following steps to customize these settings.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 vfi vfi-name autodiscovery**
4. **vpn id vpn-id**
5. **vpls-id {autonomous-system-number:nn | ip-address:nn}**
6. **rd {autonomous-system-number:nn | ip-address:nn}**
7. **route-target [import | export | both] {autonomous-system-number:nn | ip-address:nn}**
8. **l2 router-id ip-address**
9. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                              | Purpose                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <pre>configure terminal</pre> <p><b>Example:</b><br/>Router# configure terminal</p>                            | Enters global configuration mode.                                                                                  |
| Step 3 | <pre>l2 vfi vfi-name autodiscovery</pre> <p><b>Example:</b><br/>Router(config)# l2 vfi vpls1 autodiscovery</p> | Enables VPLS Autodiscovery on the PE router and enters L2 VFI configuration mode.                                  |

|        | Command or Action                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>vpn id</b> <i>vpn-id</i><br><br><b>Example:</b><br>Router(config-vfi)# vpn id 10                                                                                                                   | Configures a VPN ID for the VPLS domain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 5 | <b>vpls-id</b> { <i>autonomous-system-number:nn</i>   <i>ip-address:nn</i> }<br><br><b>Example:</b><br>Router(config-vfi)# vpls-id 5:300                                                              | (Optional) Specifies the VPLS domain. This command is optional, because VPLS Autodiscovery automatically generates a VPLS ID using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated VPLS ID.<br><br>There are two formats for configuring the VPLS ID argument. It can be configured in the <i>autonomous-system-number:network number (ASN:nn)</i> format, as shown in the example, or it can be configured in the <i>IP-address:network number (IP-address:nn)</i> format.                                               |
| Step 6 | <b>rd</b> { <i>autonomous-system-number:nn</i>   <i>ip-address:nn</i> }<br><br><b>Example:</b><br>Router(config-vfi)# rd 2:3                                                                          | (Optional) Specifies the RD to distribute endpoint information. This command is optional, because VPLS Autodiscovery automatically generates an RD using the BGP autonomous system number and the configured VFI VPN ID. You can use this command to change the automatically generated route distinguisher.<br><br>There are two formats for configuring the route distinguisher argument. It can be configured in the <i>autonomous-system-number:network number (ASN:nn)</i> format, as shown in the example, or it can be configured in the <i>IP-address:network number (IP-address:nn)</i> format. |
| Step 7 | <b>route-target</b> [ <b>import</b>   <b>export</b>   <b>both</b> ] { <i>autonomous-system-number:nn</i>   <i>ip-address:nn</i> }<br><br><b>Example:</b><br>Router(config-vfi)# route-target 600:2222 | (Optional) Specifies the route target (RT). This command is optional, because VPLS Autodiscovery automatically generates a route target using the lower 6 bytes of the RD and VPLS ID. You can use this command to change the automatically generated route target.<br><br>There are two formats for configuring the route target argument. It can be configured in the <i>autonomous-system-number:network number (ASN:nn)</i> format, as shown in the example, or it can be configured in the <i>IP-address:network number (IP-address:nn)</i> format.                                                 |
| Step 8 | <b>12 router-id</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-vfi)# 12 router-id 10.10.10.10                                                                                          | (Optional) Specifies a unique identifier for the PE router. This command is optional, because VPLS Autodiscovery automatically generates a Layer 2 router ID using the MPLS global router ID. You can use this command to change the automatically generated ID.                                                                                                                                                                                                                                                                                                                                         |
| Step 9 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vfi)# exit                                                                                                                                        | Exits L2 VFI configuration mode. Commands take effect after the router exits L2 VFI configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



# Configuration Examples for VPLS Autodiscovery: BGP Based

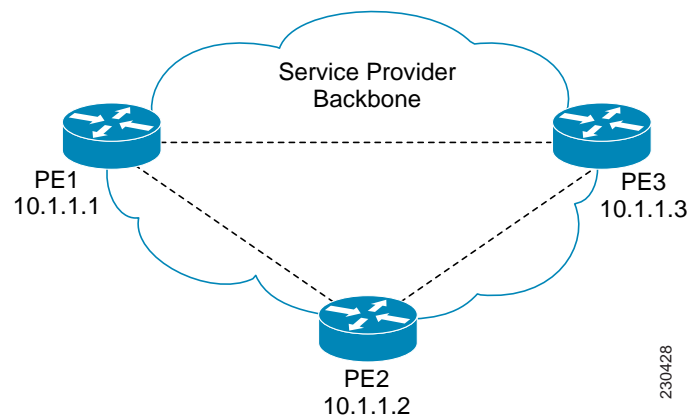
The following examples show the configuration of a network using VPLS Autodiscovery and VPLS Autodiscovery supported on a route reflector:

- [VPLS Autodiscovery: BGP Based: Basic Example, page 11](#)
- [BGP VPLS Autodiscovery Support on Route Reflector: Example, page 13](#)

## VPLS Autodiscovery: BGP Based: Basic Example

Figure 1 shows a basic configuration of VPLS Autodiscovery.

**Figure 1 Basic VPLS Autodiscovery Configuration**



### PE1

```

l2 router-id 10.1.1.1
l2 vfi auto autodiscovery
  vpn id 100
!
pseudowire-class mpls
  encapsulation mpls
!
interface Loopback1
  ip address 10.1.1.1 255.255.255.255
!
interface Ethernet0/0
  description Backbone interface
  ip address 192.168.0.1 255.255.255.0
  mpls ip
!
router ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  bgp update-delay 1

```

```

neighbor 10.1.1.2 remote-as 1
neighbor 10.1.1.2 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.1.1.2 activate
neighbor 10.1.1.2 send-community extended
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community extended
exit-address-family

```

## PE2

```

l2 router-id 10.1.1.2
l2 vfi auto autodiscovery
   vpn id 100
!
pseudowire-class mpls
encapsulation mpls
!
interface Loopback1
ip address 10.1.1.2 255.255.255.255
!
interface Ethernet0/0
description Backbone interface
ip address 192.168.0.2 255.255.255.0
mpls ip
!
router ospf 1
log-adjacency-changes
network 10.1.1.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.1.1.1 remote-as 1
neighbor 10.1.1.1 update-source Loopback1
neighbor 10.1.1.3 remote-as 1
neighbor 10.1.1.3 update-source Loopback1
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.1.1.1 activate
neighbor 10.1.1.1 send-community extended
neighbor 10.1.1.3 activate
neighbor 10.1.1.3 send-community extended
exit-address-family

```

**PE3**

```

12 router-id 10.1.1.3
12 vfi auto autodiscovery
   vpn id 100
!
pseudowire-class mpls
  encapsulation mpls
!
interface Loopback1
  ip address 10.1.1.3 255.255.255.255
!
interface Ethernet0/0
  description Backbone interface
  ip address 192.168.0.3 255.255.255.0
  mpls ip
!
router ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.0.0 0.0.0.255 area 0
!
router bgp 1
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  bgp update-delay 1
  neighbor 10.1.1.1 remote-as 1
  neighbor 10.1.1.1 update-source Loopback1
  neighbor 10.1.1.2 remote-as 1
  neighbor 10.1.1.2 update-source Loopback1
!
  address-family ipv4
    no synchronization
    no auto-summary
    exit-address-family
  !
  address-family l2vpn vpls
    neighbor 10.1.1.1 activate
    neighbor 10.1.1.1 send-community extended
    neighbor 10.1.1.2 activate
    neighbor 10.1.1.2 send-community extended
    exit-address-family

```

**BGP VPLS Autodiscovery Support on Route Reflector: Example**

In the following example, a host named PE-RR (indicating Provider Edge-Route Reflector) is configured as a route reflector capable of reflecting VPLS prefixes. The VPLS address family is configured by **address-family l2vpn vpls** below.

```

hostname PE-RR
!
router bgp 1
  bgp router-id 1.1.1.3
  no bgp default route-target filter
  bgp log-neighbor-changes
  neighbor iBGP_PEERS peer-group
  neighbor iBGP_PEERS remote-as 1
  neighbor iBGP_PEERS update-source Loopback1
  neighbor 1.1.1.1 peer-group iBGP_PEERS
  neighbor 1.1.1.2 peer-group iBGP_PEERS
!

```

```

address-family l2vpn vpls
  neighbor iBGP_PEERS send-community extended
  neighbor iBGP_PEERS route-reflector-client
  neighbor 1.1.1.1 peer-group iBGP_PEERS
  neighbor 1.1.1.2 peer-group iBGP_PEERS
exit-address-family

```

## Additional References

The following sections provide references related to the VPLS Autodiscovery: BGP Based feature.

## Related Documents

| Related Topic                                                | Document Title                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Virtual Private LAN Services on the Cisco 7600 series router | “Virtual Private LAN Services on the Optical Services Modules” chapter in the <i>Cisco 7600 Series Router Cisco IOS Software Configuration Guide</i> , Release 12.2SR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| L2 VPNs on the Cisco 7600 router                             | Configuration information for Layer 2 VPNs on the Cisco 7600 router is included in the following documents: <ul style="list-style-type: none"> <li>The “Configuring PFC3BXL and PFC3B Mode Multiprotocol Label Switching” module of the <i>Cisco 7600 Series Cisco IOS Software Configuration Guide</i>, Release 12.2SR</li> <li>The “Configuring Multiprotocol Label Switching on the Optical Services Modules” module of the <i>OSM Configuration Note</i>, Release 12.2SR</li> <li>The “Configuring Multiprotocol Label Switching on FlexWAN and Enhanced FlexWAN Modules” module of the <i>FlexWAN and Enhanced FlexWAN Modules Configuration Guide</i></li> <li>The “Configuring Any Transport over MPLS on a SIP” section of the <i>Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</i></li> <li>The “Configuring AToM VP Cell Mode Relay Support” section of the <i>Cisco 7600 Series Router SIP, SSC, and SPA Software Configuration Guide</i></li> <li>The <i>Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers</i></li> </ul> |
| MPLS Commands                                                | <i>Cisco IOS Multiprotocol Label Switching Command Reference</i><br><a href="http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html">http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Standards

| Standard                          | Title                                                                               |
|-----------------------------------|-------------------------------------------------------------------------------------|
| draft-ietf-l2vpn-signaling-08.txt | <i>Provisioning, Autodiscovery, and Signaling in L2VPNs</i>                         |
| draft-ietf-l2vpn-vpls-bgp-08.8    | <i>Virtual Private LAN Service (VPLS) Using BGP for Autodiscovery and Signaling</i> |
| draft-ietf-mpls-lsp-ping-03.txt   | <i>Detecting MPLS Data Plane Failures</i>                                           |
| draft-ietf-pwe3-vccv-01.txt       | <i>Pseudo-Wire (PW) Virtual Circuit Connection Verification (VCCV)</i>              |

## MIBs

| MIB                                                                                                                                                                                                                                                            | MIBs Link                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>CISCO-IETF-PW-MIB (PW-MIB)</li> <li>CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB)</li> <li>CISCO-IETF-PW-ENET-MIB (PW-ENET-MIB)</li> <li>CISCO-IETF-PW-FR-MIB (PW-FR-MIB)</li> <li>CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB)</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                                                             |
|----------|-------------------------------------------------------------------|
| RFC 3916 | <i>Requirements for Pseudo-wire Emulation Edge-to-Edge (PWE3)</i> |
| RFC 3981 | <i>Pseudo Wire Emulation Edge-to-Edge Architecture</i>            |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                              | Link                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for VPLS Autodiscovery: BGP Based

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for VPLS Autodiscovery: BGP Based

| Feature Name                                      | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VPLS Autodiscovery: BGP Based                     | 12.2(33)SRB | <p>VPLS Autodiscovery enables each Virtual Private LAN Service (VPLS) provider edge (PE) router to discover which other PE routers are part of the same VPLS domain.</p> <p>In 12.2(33)SRB, this feature was introduced on the Cisco 7600 router.</p> <p>The following commands were introduced or modified for this feature:</p> <ul style="list-style-type: none"> <li>• <b>auto-route-target</b></li> <li>• <b>l2 router-id</b></li> <li>• <b>l2 vfi autodiscovery</b></li> <li>• <b>neighbor (VPLS)</b></li> <li>• <b>rd (VPLS)</b></li> <li>• <b>route-target (VPLS)</b></li> <li>• <b>show mpls l2transport vc</b></li> <li>• <b>show vfi</b></li> <li>• <b>show xconnect</b></li> <li>• <b>vpls-id</b></li> <li>• <b>xconnect</b></li> </ul> |
| BGP VPLS Autodiscovery Support on Route Reflector | 12.2(33)SRE | <p>This feature was introduced on the Cisco 7600 series routers. This feature is documented in the following sections:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP VPLS Autodiscovery Support on a Route Reflector, page 4</a></li> <li>• <a href="#">BGP VPLS Autodiscovery Support on Route Reflector: Example, page 13</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                           |

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

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

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.







# H-VPLS N-PE Redundancy for QinQ and MPLS Access

---

**First Published: November 15, 2007**

**Last Updated: December 21, 2007**

The H-VPLS N-PE Redundancy for QinQ and MPLS Access feature enables two network provider edge (N-PE) routers to provide failover services to a user provider edge (U-PE) router in a hierarchical virtual private LAN service (H-VPLS). Having redundant N-PE routers provides improved stability and reliability against link and node failures. This document explains how to implement this feature.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for H-VPLS N-PE Redundancy for QinQ and MPLS Access](#)” section on page 13.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for H-VPLS N-PE Redundancy for QinQ and MPLS Access](#), page 2
- [Restrictions for H-VPLS N-PE Redundancy for QinQ and MPLS Access](#), page 2
- [Information About H-VPLS N-PE Redundancy for QinQ and MPLS Access](#), page 3
- [How to Configure H-VPLS N-PE Redundancy for QinQ and MPLS Access](#), page 6
- [Configuration Examples for H-VPLS N-PE Redundancy for QinQ and MPLS Access](#), page 9
- [Additional References](#), page 11
- [Command Reference](#), page 12



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [Feature Information for H-VPLS N-PE Redundancy for QinQ and MPLS Access, page 13](#)
- [Glossary, page 14](#)

## Prerequisites for H-VPLS N-PE Redundancy for QinQ and MPLS Access

- Before configuring the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature, configure your H-VPLS network and make sure it is operating correctly. For more information about configuring the H-VPLS network, see the “Configuring VPLS” chapter of the [Configuring Multiprotocol Label Switching on the Optical Services Modules](#).
- Make sure that the PE-to-CE interface is configured the switchport trunk with a list of allowed VLANs. For more information, see the “Configuring VPLS” chapter of the “Configuring VPLS” chapter of the [Configuring Multiprotocol Label Switching on the Optical Services Modules](#).
- To provide faster convergence, you can optionally enable the MPLS Traffic Engineering: Fast Reroute feature in the Multiprotocol Label Switching (MPLS) core. See the [MPLS Traffic Engineering \(TE\)—Fast Reroute \(FRR\) Link and Node Protection](#) documentation.
- Enable the L2VPN Pseudowire Redundancy feature on the U-PE routers for MPLS access. For information about configuring the L2VPN Pseudowire Redundancy feature, see the [L2VPN Pseudowire Redundancy](#) documentation.

- When configuring MSTP, specify that one of N-PEs routers is the root by assigning it the lowest priority, using the following command:

```
spanning-tree mst instance-id priority priority
```

For information about configuring MSTP, see the “Configuring MST Instance Parameters” chapter of the [Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.1E](#).

- When configuring MSTP, make sure each of the routers participating in the spanning-tree are in the same region and are the same revision by issuing the **revision**, **name**, and **instance** commands in MST configuration mode. For more information on configuring these MSTP parameters, see the “Configuring IEEE 802.1s MST” chapter of the [Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.1E](#).

## Restrictions for H-VPLS N-PE Redundancy for QinQ and MPLS Access

- H-VPLS N-PE Redundancy for QinQ and MPLS Access cannot be used with the VPLS Autodiscovery feature on the pseudowires that attach to the U-PE routers. When you create the VPLS, manually create the virtual forwarding interface (VFI).
- You cannot configure more than one pseudowire (PW) to carry the bridge protocol data unit (BPDU) information between the N-PE routers. If you attempt to enter the **forward permit l2protocol all** command for multiple VFIs, you receive an error message.
- You cannot configure a local loopback address as a neighbor when you configure the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature on the N-PE routers. If you do, the following error is displayed:

```
VPLS local switching to peer address not supported
```

- Only two N-PE routers can be connected to each U-PE router.
- For a list of supported hardware for this feature, see the [Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers](#).
- The spanning tree mode must be MSTP for the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature. If the spanning tree mode changes, the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature may not work correctly, even though the pseudowire that carries the BPDUs information still exists and the H-VPLS N-PE Redundancy is still configured.

## Information About H-VPLS N-PE Redundancy for QinQ and MPLS Access

Before configuring the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature, you should understand the following concepts:

- [How H-VPLS N-PE Redundancy for QinQ and MPLS Access Works](#), page 3
- [MAC Address Withdrawal](#), page 5

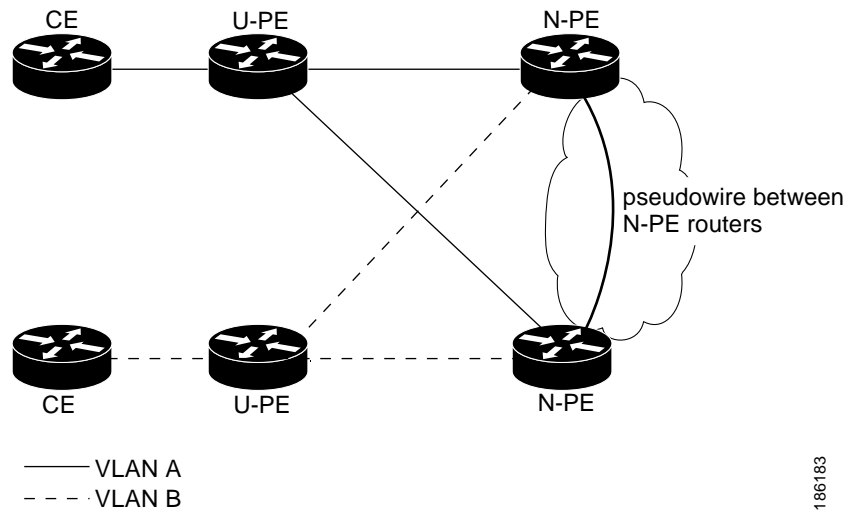
## How H-VPLS N-PE Redundancy for QinQ and MPLS Access Works

In a network configured with the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature, the U-PE router is connected to two N-PE routers, which provides a level of redundancy that can tolerate both link or device faults. If a failure occurs in the network that disables one N-PE router from transmitting data, the other N-PE router will take over. This feature works with both QinQ access based on Multiple Spanning Tree Protocol (MSTP) and MPLS access based on pseudowire redundancy.

### H-VPLS N-PE Redundancy with QinQ Access Based on MSTP

H-VPLS N-PE redundancy with QinQ access uses MSTP running on the N-PE routers and U-PE routers in an H-VPLS network. A pseudowire running between N-PE routers carries only MSTP BPDUs. The pseudowire running between the N-PE routers is always up and is used to create a loop path between N-PE routers so that MSTP will block one of the redundant paths between the U-PE router and the N-PE routers. If the primary N-PE router or the path to it fails, MSTP will enable the path to the backup N-PE router.

[Figure 1](#) shows an H-VPLS network with redundant access. Each U-PE router has two trunk connections, one to each N-PE router. Between the two N-PE routers is a pseudowire to provide a loop path for MSTP BPDUs. The network topology shown in [Figure 1](#) allows for the backup N-PE router to take over if the primary N-PE router or the path to it fails.

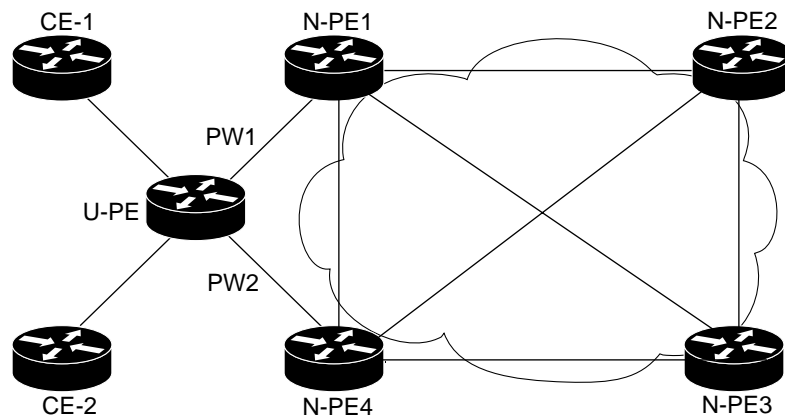
**Figure 1** *H-VPLS N-PE Redundancy with QinQ access Based on MSTP*

186183

## H-VPLS N-PE Redundancy with MPLS Access Based on Pseudowire Redundancy

For H-VPLS redundancy with MPLS access based on pseudowire redundancy, the MPLS network has pseudowires to the VPLS core N-PE routers.

As shown in [Figure 2](#), one pseudowire transports data between the U-PE router and its peer N-PE routers. When a failure occurs along the path of the U-PE router, the backup pseudowire and the redundant N-PE router become active and start transporting data.

**Figure 2** *H-VPLS N-PE Redundancy for QinQ and MPLS Access with MPLS Access Based On Pseudowire Redundancy*

186184

## MAC Address Withdrawal

PE routers learn the remote MAC addresses and directly attached MAC addresses on customer-facing ports by deriving topology and forwarding information from packets originating at customer sites. To display the number of MAC address withdrawal messages, enter the **show mpls l2transport vc detail** command, as shown in the following example. The MAC address withdrawal message is shown in bold.

```
Router# show mpls l2transport vc detail

Local interface: VFI TEST VFI up
MPLS VC type is VFI, interworking type is Ethernet
Destination address: 10.1.1.1, VC ID: 1000, VC status: up
Output interface: Se2/0, imposed label stack {17}
Preferred path: not configured
Default path: active
Next hop: point2point
Create time: 00:04:34, last status change time: 00:04:15
Signaling protocol: LDP, peer 10.1.1.1:0 up
Targeted Hello: 10.1.1.1(LDP Id) -> 10.1.1.1
MPLS VC labels: local 16, remote 17
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
MAC Withdraw: sent 5, received 3
Sequencing: receive disabled, send disabled
VC statistics:
packet totals: receive 0, send 0
byte totals:   receive 0, send 0
packet drops:  receive 0, send 0
```

### How MAC Address Withdrawal Works with H-VPLS N-PE Redundancy with QinQ Access

If a failure occurs in the customer switched network, a spanning tree Topology Change Notification (TCN) is issued to the U-PE router, which issues an LDP-based MAC address withdrawal message to the peer N-PE routers and flushes its MAC address table.

### How MAC Address Withdrawal Works with H-VPLS N-PE Redundancy with MPLS Access

If the pseudowire between the U-PE router and N-PE router fails, then the L2VPN Pseudowire Redundancy feature on the U-PE router activates the standby pseudowire. In addition, the U-PE router sends a Label Distribution Protocol (LDP) MAC address withdrawal request to the new N-PE router, which forwards the message to all pseudowires in the VPLS core and flushes its MAC address table.

If a switched virtual interface (SVI) on the N-PE router fails, the L2VPN Pseudowire Redundancy feature activates the standby pseudowire and the U-PE router sends a MAC withdrawal message to the newly active N-PE router.

For information about the L2VPN Pseudowire Redundancy feature, see the [L2VPN Pseudowire Redundancy](#) feature.

# How to Configure H-VPLS N-PE Redundancy for QinQ and MPLS Access

This section contains the following procedures:

- [Configuring the VPLS Pseudowire Between the N-PE Routers, page 6](#) (required)
- [Configuring the SVI for the Native VLAN, page 7](#) (required)
- [Verifying the H-VPLS N-PE Redundancy for QinQ and MPLS Access Configuration, page 8](#) (optional)

## Configuring the VPLS Pseudowire Between the N-PE Routers

Configuring N-PE redundancy in an H-VPLS network requires two steps. First you define the VPLS pseudowire for transporting BPDU data. Then, you connect that pseudowire to the native VLAN. This provides a redundancy that provides improved reliability against link and node failures.

### Prerequisites

- Before configuring the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature, configure your H-VPLS network and make sure it is operating correctly. For more information about configuring the H-VPLS network, see the “Configuring VPLS” chapter of the [Configuring Multiprotocol Label Switching on the Optical Services Modules](#).
- Make sure that the PE-to-CE interface is configured the switchport trunk with a list of allowed VLANs. For more information, see the “Configuring VPLS” chapter of the “Configuring VPLS” chapter of the [Configuring Multiprotocol Label Switching on the Optical Services Modules](#).
- To provide faster convergence, you can optionally enable the MPLS Traffic Engineering: Fast Reroute feature in the Multiprotocol Label Switching (MPLS) core. See the [MPLS Traffic Engineering \(TE\)—Fast Reroute \(FRR\) Link and Node Protection](#) documentation.
- Enable the L2VPN Pseudowire Redundancy feature on the U-PE routers for MPLS access. For information about configuring the L2VPN Pseudowire Redundancy feature, see the [L2VPN Pseudowire Redundancy](#) documentation.
- When configuring MSTP, specify that one of N-PEs routers is the root by assigning it the lowest priority, using the following command:

**spanning-tree mst instance-id priority priority**

For information about configuring MSTP, see the “Configuring MST Instance Parameters” chapter of the [Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.1E](#).

- When configuring MSTP, make sure each of the routers participating in the spanning-tree are in the same region and are the same revision by issuing the **revision**, **name**, and **instance** commands in MST configuration mode. For more information on configuring these MSTP parameters, see the “Configuring IEEE 802.1s MST” chapter of the [Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.1E](#).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **l2 vfi** *name* **manual**
4. **vpn id** *id-number*
5. **forward permit l2protocol all**
6. **neighbor** *remote-router-id* *vc-id* {**encapsulation** *encapsulation-type* | **pw-class** *pw-name*}  
[**no-split-horizon**]
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                               | Purpose                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                  | Enters global configuration mode.                                                                                        |
| Step 3 | <b>l2 vfi</b> <i>name</i> <b>manual</b><br><br><b>Example:</b><br>Router(config)# l2 vfi vfitest1 manual                                                                                                                                                        | Creates a Layer 2 VFI and enters Layer 2 VFI manual configuration mode.                                                  |
| Step 4 | <b>vpn id</b> <i>id-number</i><br><br><b>Example:</b><br>Router(config-vfi)# vpn id 200                                                                                                                                                                         | Specifies the VPN ID.                                                                                                    |
| Step 5 | <b>forward permit l2protocol all</b><br><br><b>Example:</b><br>Router(config-vfi)# forward permit l2protocol all                                                                                                                                                | Creates a pseudowire that is to be used to transport BPDU data between the two N-PE routers.                             |
| Step 6 | <b>neighbor</b> <i>remote-router-id</i> <i>vc-id</i> { <b>encapsulation</b> <i>encapsulation-type</i>   <b>pw-class</b> <i>pw-name</i> }<br>[ <b>no-split-horizon</b> ]<br><br><b>Example:</b><br>Router(config-vfi)# neighbor 10.2.2.2 3<br>encapsulation mpls | Specifies the peer IP address of the redundant N-PE router and the type of tunnel signaling and encapsulation mechanism. |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-vfi)# end                                                                                                                                                                                                    | Ends the current configuration session and returns to privileged EXEC mode.                                              |

## Configuring the SVI for the Native VLAN

Perform the following task to configure the switch virtual interface for the native VLAN.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **interface vlan** *vlanid*
4. **xconnect vfi** *vfi-name*

**DETAILED STEPS**

|        | Command or Action                                                                                   | Purpose                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                   |
| Step 3 | <b>interface vlan</b> <i>vlanid</i><br><br><b>Example:</b><br>Router(config)# interface vlan 23     | Creates a dynamic SVI.                                                                                              |
| Step 4 | <b>xconnect vfi</b> <i>vfi-name</i><br><br><b>Example:</b><br>Router(config)# xconnect vfi vfitest1 | Specifies the Layer 2 VFI that you are binding to the VLAN port.                                                    |

## Verifying the H-VPLS N-PE Redundancy for QinQ and MPLS Access Configuration

To ensure that the H-VPLS N-PE Redundancy for QinQ and MPLS Access feature is correctly configured, perform the following task.

**SUMMARY STEPS**

1. **show vfi** *vfi-name*

**DETAILED STEPS****Step 1** **show vfi** *vfi-name*

Use this command on the pseudowire between the two N-PE routers to displays information about the pseudowire, as shown in the following example:

```
Router# show vfi VPLS-2
```

```
VFI name: VPLS-2, state: up
VPN ID: 100
```



```

Local attachment circuits:
  Vlan2
Neighbors connected via pseudowires:
Peer Address      VC ID      Split-horizon
10.1.1.1          2          Y
10.1.1.2          2          Y
10.2.2.3          2          N

```

## Configuration Examples for H-VPLS N-PE Redundancy for QinQ and MPLS Access

This section provides the following example for configuring H-VPLS redundancy:

- [H-VPLS N-PE Redundancy for QinQ Access: Example](#)

### H-VPLS N-PE Redundancy for QinQ Access: Example

Figure 3 shows a configuration that is set up for H-VPLS N-PE redundancy with QinQ access.

**Figure 3** H-VPLS N-PE Redundancy with QinQ Access Topology

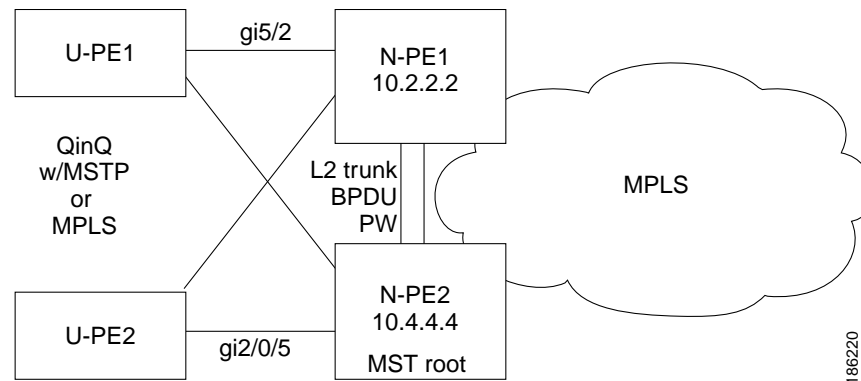


Table 1 shows the configuration of two N-PE routers for H-VPLS N-PE redundancy with QinQ access.

**Table 1** H-VPLS N-PE Redundancy for QinQ Access: Example

| N-PE1                                                                                                                                                                                                                                                                                                                                                                                                                                                     | N-PE2                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> 12 vfi l2trunk manual   vpn id 10   forward permit l2protocol all   neighbor 10.4.4.4 encapsulation mpls ! interface Vlan1   no ip address   xconnect vfi l2trunk ! spanning-tree mode mst spanning-tree extend system-id ! spanning-tree mst configuration   revision 10   instance 1 vlan 20 ! interface GigabitEthernet5/2   switchport   switchport trunk encapsulation dot1q   switchport trunk allowed vlan 20   switchport mode trunk </pre> | <pre> 12 vfi l2trunk manual   vpn id 10   forward permit l2protocol all   neighbor 10.2.2.2 encapsulation mpls ! interface Vlan1   no ip address   xconnect vfi l2trunk ! spanning-tree mode mst spanning-tree extend system-id ! spanning-tree mst configuration   revision 10   instance 1 vlan 20 ! spanning-tree mst 1 priority 0 ! interface GigabitEthernet2/0/5   switchport   switchport trunk allowed vlan 20   switchport mode trunk   mls qos trust dscp </pre> |

# Additional References

The following sections provide references related to the H-VPLS N-PE Redundancy feature.

## Related Documents

| Related Topic                                       | Document Title                                                                                                              |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| L2VPN pseudowire redundancy                         | <a href="#">L2VPN Pseudowire Redundancy</a>                                                                                 |
| H-VPLS                                              | “Configuring VPLS” chapter of the <i>Configuring Multiprotocol Label Switching on the Optical Services Modules</i>          |
| Multiple spanning tree configuration                | “Configuring MST Instance Parameters” chapter of the <i>Cisco 7600 Series Cisco IOS Software Configuration Guide, 12.1E</i> |
| MPLS traffic engineering                            | <i>MPLS Traffic Engineering (TE)—Fast Reroute (FRR) Link and Node Protection</i>                                            |
| Supported hardware on the Cisco 7600 series routers | <i>Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers</i>                                         |

## Standards

| Standard                                                                                                                                                              | Title                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| <a href="http://www.ietf.org/rfc/rfc4447.txt">http://www.ietf.org/rfc/rfc4447.txt</a>                                                                                 | Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) |
| <a href="http://www3.ietf.org/proceedings/06mar/IDs/draft-ietf-l2vpn-vpls-ldp-08.txt">http://www3.ietf.org/proceedings/06mar/IDs/draft-ietf-l2vpn-vpls-ldp-08.txt</a> | Virtual Private LAN Services over MPLS                                       |
| <a href="http://www.ietf.org/internet-drafts/draft-ietf-pwe3-segmented-pw-02.txt">http://www.ietf.org/internet-drafts/draft-ietf-pwe3-segmented-pw-02.txt</a>         | Segmented Pseudo Wire                                                        |
| <a href="#">draft-ietf-pwe3-vccv-10.txt</a>                                                                                                                           | Pseudo Wire Virtual Circuit Connectivity Verification (VCCV)                 |
| <a href="#">draft-ietf-pwe3-oam-msg-map-03.txt</a>                                                                                                                    | Pseudo Wire (PW) OAM Message Mapping                                         |

## MIBs

| MIB                                                                                | MIBs Link                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module.

- **forward permit l2protocol**
- **show mpls l2transport vc**

For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html).

For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the Cisco IOS Master Commands List.

# Feature Information for H-VPLS N-PE Redundancy for QinQ and MPLS Access

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for H-VPLS N-PE Redundancy for QinQ and MPLS Access

| Feature Name                                    | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| H-VPLS N-PE Redundancy for QinQ and MPLS Access | 12.2(33)SRC | <p>The H-VPLS N-PE Redundancy for QinQ and MPLS Access feature enables two network provider edge (N-PE) routers to provide redundancy to a user provider edge (U-PE) router in a hierarchical virtual private LAN service (VPLS). Having redundant N-PE routers provides improved stability and reliability against link and node failures.</p> <p>In Release 12.2(33)SRC, this feature was introduced on the Cisco Series 7600 router.</p> <p>The following commands were introduced or modified by this feature: <b>forward permit l2protocol</b> and <b>show mpls l2transport vc</b>.</p> |

# Glossary

**CE router**—Customer edge router. A router that belongs to a customer network, which connects to a PE router to utilize MPLS VPN network services.

**LAN**—Local area network. High-speed, low-error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.

**MPLS**—Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**MSTP**—Multiple Spanning Tree Protocol. The MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs.

**PE router**—Provider edge router. The PE router is the entry point into the Service Provider network. The PE router is typically deployed on the edge of the network and is administered by the Service Provider.

**PW**—Pseudowire.

**N-PE**—Network-facing PE router. This router acts as a gateway between the MPLS core and edge domains.

**pseudowire**—A pseudowire is a virtual connection that, in the context of VPLS, connects two VSIs. A pseudowire is bidirectional and consists of a pair of uni-directional MPLS Virtual Circuits (VCs). A pseudowire can be used to connect a point-to-point circuit.

**PW**—Pseudowire. A mechanism that carries the elements of an emulated service from one PE router to one or more PEs over a packet switched network (PSN).

**QinQ**—An IEEE 802.1Q VLAN tunnel.

**redundancy**—The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

**router**—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**U-PE**—Customer-facing PE router. This router connects Customer Edge (CE) routers to the service.

**QinQ**—A mechanism for constructing multipoint Layer 2 VPN using Ethernet switches.

**spanning tree**—Loop-free subset of a network topology.

**VFI**—Virtual forwarding instance. A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more VCs.

**VLAN**—Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

**VPLS**—Virtual Private LAN Service. VPLS describes an architecture that delivers Layer 2 service that emulates an Ethernet LAN across a Wide Area Network (WAN) and inherits the scaling characteristics of a LAN.

**VPLS redundancy**—Also called N-PE redundancy. Allows U-PEs to be dual-homed (to their N-PEs) in a loop-free topology with MPLS or QinQ as the access or aggregation domain.

**VPN**—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

---

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

© 2007 Cisco Systems, Inc. All rights reserved.







# L2VPN Multisegment Pseudowires

---

**First Published: February 27, 2009**

**Last Updated: November 20, 2009**

The L2VPN Multisegment Pseudowires feature enables you to configure two or more Layer 2 pseudowire segments that function as a single pseudowire. The feature spans multiple cores or autonomous systems of the same or different carrier networks.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for L2VPN Multisegment Pseudowires”](#) section on page 12.

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

## Contents

- [Prerequisites for L2VPN Multisegment Pseudowires, page 2](#)
- [Restrictions for L2VPN Multisegment Pseudowires, page 2](#)
- [Information About L2VPN Multisegment Pseudowires, page 2](#)
- [How to Configure L2VPN Multisegment Pseudowires, page 4](#)
- [Additional References, page 10](#)
- [Feature Information for L2VPN Multisegment Pseudowires, page 12](#)



---

**Americas Headquarters:**

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

© 2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for L2VPN Multisegment Pseudowires

Before configuring this feature, see the following documents:

- [Any Transport over MPLS](#)
- [L2VPN Pseudowire Switching](#)
- [MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV](#)
- [Pseudowire Setup and Maintenance Using the Label Distribution Protocol \(LDP\)](#) (RFC 4447)

## Restrictions for L2VPN Multisegment Pseudowires

- Only Multiprotocol Label Switching (MPLS) Layer 2 pseudowires are supported.
- Only manual configuration of the pseudowires (including S-PE and T-PE routers) is supported.
- The L2VPN Pseudowire Switching feature is supported for pseudowires advertised with FEC 128. FEC 129 is not supported. See the [“Restrictions” section on page 8](#) for specific restrictions on ping mpls and trace mpls operations.
- The S-PE router is limited to 1600 pseudowires.

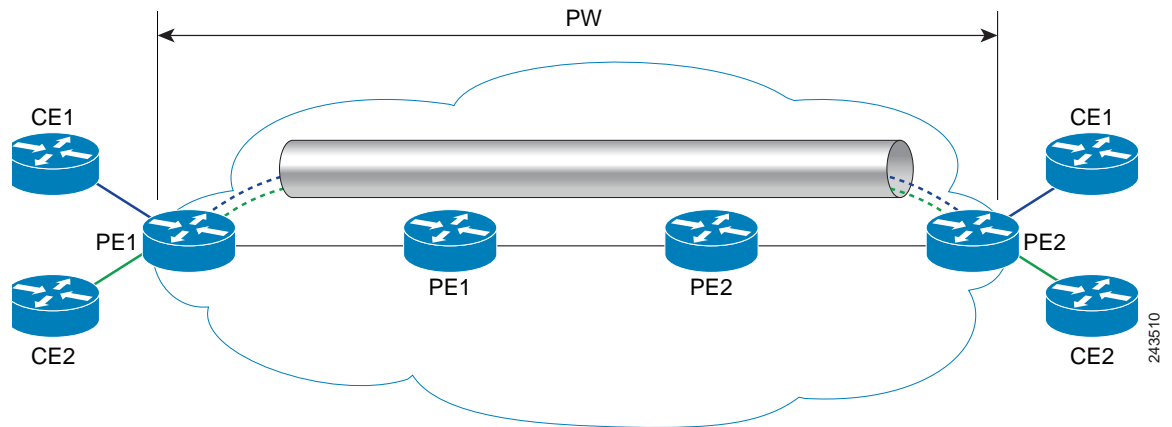
## Information About L2VPN Multisegment Pseudowires

Before configuring the L2VPN Multisegment Pseudowires feature, you should understand the following concepts:

- [L2VPN Pseudowire Defined, page 2](#)
- [L2VPN Multisegment Pseudowire Defined, page 3](#)

## L2VPN Pseudowire Defined

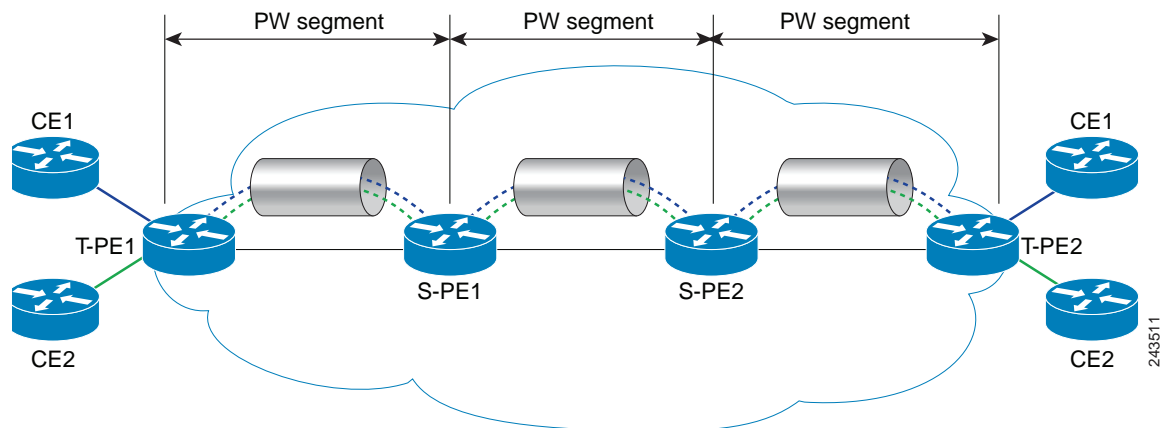
An L2VPN pseudowire (PW) is a tunnel established between two provider edge (PE) routers across the core carrying the Layer 2 payload encapsulated as MPLS data, as shown in [Figure 1](#). This helps carriers migrate from traditional Layer 2 networks such as Frame Relay and ATM to an MPLS core. In the L2VPN pseudowire shown in [Figure 2](#), the PWs between two PE routers are located within the same autonomous system. Routers PE1 and PE2 are called terminating PE routers (T-PEs). Attachment circuits are bounded to the PW on these PE routers.

**Figure 1** *An L2VPN Pseudowire*

## L2VPN Multisegment Pseudowire Defined

An L2VPN multisegment pseudowire (MS-PW) is a set of two or more PW segments that function as a single PW. It is also known as switched PW. MS-PWs span multiple cores or autonomous systems of the same or different carrier networks. An L2VPN MS-PW can include up to 254 PW segments.

The end routers are called terminating PE routers (T-PEs), and the switching routers are called S-PE routers. The S-PE router terminates the tunnels of the preceding and succeeding PW segments in an MS-PW. The S-PE router can switch the control and data planes of the preceding and succeeding PW segments of the MS-PW. An MS-PW is declared to be up when all the single-segment PWs are up. For more information, see the [L2VPN Pseudowire Switching](#) document.

**Figure 2** *A Multisegment Pseudowire*

# How to Configure L2VPN Multisegment Pseudowires

The following sections outline the tasks for creating and maintaining L2VPN multisegment pseudowires:

- [Configuring L2VPN Multisegment Pseudowires, page 4](#) (required)
- [Displaying Information About the L2VPN Multisegment Pseudowires, page 6](#) (optional)
- [Performing ping mpls and trace mpls Operations on L2VPN Multisegment Pseudowires, page 7](#) (optional)

## Configuring L2VPN Multisegment Pseudowires

Perform the following steps on the S-PE routers to create L2VPN multisegment pseudowires.

### Cisco 7600 Router-Specific Instructions

If the Cisco 7600 router is the penultimate hop router connected to the S-PE or T-PE router, issue the following commands on the S-PE or T-PE routers:

- **mpls ldp explicit-null**
- **no mls mpls explicit-null propagate-ttl**

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label protocol ldp**
4. **mpls ldp router-id *interface* force**
5. **pseudowire-class *name***
6. **encapsulation mpls**
7. **switching tlv**
8. **exit**
9. **l2 vfi *name* point-to-point**
10. **description *string***
11. **neighbor *ip-address* *vcid* {encapsulation mpls | pw-class *pw-class-name*}**

## DETAILED STEPS

|        | Command or Action                                                                                                      | Purpose                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                         | Enters global configuration mode.                                                                                                                                                                  |
| Step 3 | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp                       | Configures the use of Label Distribution Protocol (LDP) on all interfaces.                                                                                                                         |
| Step 4 | <b>mpls ldp router-id interface force</b><br><br><b>Example:</b><br>Router(config)# mpls ldp router-id loopback0 force | Specifies the preferred interface for determining the LDP router ID.                                                                                                                               |
| Step 5 | <b>pseudowire-class name</b><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom                           | Establishes a pseudowire class with a name that you specify, and enters pseudowire class configuration mode.                                                                                       |
| Step 6 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw-class)# encapsulation mpls                        | Specifies the tunneling encapsulation. <ul style="list-style-type: none"> <li>For MPLS L2VPNs, the encapsulation type is <b>mpls</b>.</li> </ul>                                                   |
| Step 7 | <b>switching tlv</b><br><br><b>Example:</b><br>Router(config-pw-class)# switching tlv                                  | (Optional) Enables the advertisement of the switching point type-length variable (TLV) in the label binding. <ul style="list-style-type: none"> <li>This command is enabled by default.</li> </ul> |
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-pw-class)# exit                                                    | Exits pseudowire class configuration mode.                                                                                                                                                         |
| Step 9 | <b>l2 vfi name point-to-point</b><br><br><b>Example:</b><br>Router(config)# l2 vfi atomtunnel point-to-point           | Creates a point-to-point Layer 2 virtual forwarding interface (VFI) and enters VFI configuration mode.                                                                                             |

|                | Command or Action                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                          |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 10</b> | <b>description</b> <i>string</i><br><br><b>Example:</b><br>Router(config-vfi)# <b>description</b> segment1                                                                                                            | Provides a description of the switching provider edge router for a multisegment pseudowire.                                                                                                                                                                                                                      |
| <b>Step 11</b> | <b>neighbor</b> <i>ip-address vcid</i><br>{ <b>encapsulation</b> <b>mpls</b>   <b>pw-class</b> <i>pw-class-name</i> }<br><br><b>Example:</b><br>Router(config-vfi)# <b>neighbor</b> 10.0.0.1 100 <b>pw-class</b> mpls | Sets up an emulated VC.<br><br><ul style="list-style-type: none"> <li>Specify the IP address and the VC ID of the peer router. Also specify the pseudowire class to use for the emulated VC.</li> </ul> <b>Note</b> Only two <b>neighbor</b> commands are allowed for each <b>l2 vfi point-to-point</b> command. |

## Displaying Information About the L2VPN Multisegment Pseudowires

Perform the following task to display the status of L2VPN multisegment pseudowires.

### SUMMARY STEPS

1. **show mpls l2transport binding**
2. **show mpls l2transport vc detail**

### DETAILED STEPS

#### Step 1 **show mpls l2transport binding**

Use the **show mpls l2transport binding** command to display information about the pseudowire switching point, as shown in bold in the output. (In the following examples PE1 and PE4 are the T-PE routers.)

Router# **show mpls l2transport binding**

```

Destination Address: 10.1.1.1,  VC ID: 102
Local Label:  17
  Cbit: 1,    VC Type: Ethernet,    GroupID: 0
  MTU: 1500,  Interface Desc: n/a
  VCCV: CC Type: CW [1], RA [2], TTL [3]
    CV Type: LSPV [2]
Remote Label: 16
  Cbit: 1,    VC Type: Ethernet,    GroupID: 0
  MTU: 1500,  Interface Desc: n/a
  VCCV: CC Type: CW [1], RA [2], TTL [3]
    CV Type: LSPV [2]
PW Switching Point:
    Vcid  local IP addr    remote IP addr    Description
    101   10.11.11.11      10.20.20.20      PW Switching Point PE3
    100   10.20.20.20      10.11.11.11      PW Switching Point PE2

```

#### Step 2 **show mpls l2transport vc detail**

Use the **show mpls l2transport vc detail** command to display status of the pseudowire switching point. In the following example, the output (shown in bold) displays the segment that is the source of the fault of the multisegment pseudowire:

```

Router# show mpls l2transport vc detail

Local interface: Se3/0 up, line protocol up, HDLC up
  Destination address: 12.1.1.1, VC ID: 100, VC status: down
  Output interface: Se2/0, imposed label stack {23}
  Preferred path: not configured
  Default path: active
  Next hop: point2point
Create time: 00:03:02, last status change time: 00:01:41
Signaling protocol: LDP, peer 10.1.1.1:0 up
  Targeted Hello: 10.1.1.4(LDP Id) -> 10.1.1.1, LDP is UP
  Status TLV support (local/remote)   : enabled/supported
    LDP route watch                   : enabled
    Label/status state machine        : established, LruRrd
  Last local dataplane status rcvd: No fault
  Last local SSS circuit status rcvd: No fault
  Last local SSS circuit status sent: DOWN(PW-tx-fault)
  Last local LDP TLV status sent: No fault
  Last remote LDP TLV status rcvd: DOWN(PW-tx-fault)
  PW Switching Point:
    Fault type Vcid local IP addr remote IP addr Description
    PW-tx-fault 101 10.1.1.1      10.1.1.1      S-PE2
  Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 19, remote 23
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description:
Sequencing: receive disabled, send disabled
VC statistics:
  packet totals: receive 16, send 27
  byte totals:   receive 2506, send 3098
  packet drops:  receive 0, seq error 0, send 0

```

## Performing ping mpls and trace mpls Operations on L2VPN Multisegment Pseudowires

You can use the **ping mpls** and **trace mpls** commands to verify that all the segments of the MPLS multisegment pseudowire are operating.

You can use the **ping mpls** command to verify connectivity at the following pseudowire points:

- From one end of the pseudowire to the other
- From one of the pseudowires to a specific segment
- The segment between two adjacent S-PE routers

You can use the **trace mpls** command to verify connectivity at the following pseudowire points:

- From one end of the pseudowire to the other
- From one of the pseudowires to a specific segment
- The segment between two adjacent S-PE routers
- A range of segments

## Restrictions

Some **ping mpls** and **trace mpls** keywords that are available with IPv4 LDP or traffic engineering (TE), are not available with pseudowire.

The following keywords are not available with the **ping mpls pseudowire** command:

- **dsmap**
- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

The following keywords are not available with the **trace mpls pseudowire** command:

- **flags**
- **force-explicit-null**
- **output**
- **revision**
- **ttl**

## SUMMARY STEPS

1. **ping mpls pseudowire** *destination-address* *vc-id* [**segment** *segment-number*]
2. **trace mpls pseudowire** *destination-address* *vc-id* **segment** *segment-number* [*segment-number*]

## DETAILED STEPS

---

**Step 1** **ping mpls pseudowire** *destination-address* *vc-id* [**segment** *segment-number*]

Where:

- *destination-address* is the address of the S-PE router, which is the end of the segment from the direction of the source.
- *vc-id* is the VC ID of the segment from the source to the next PE router.
- **segment** *segment-number* is optional and specifies the segment you want to ping.

The following examples use the topology shown in [Figure 2](#):

- To perform an end-to-end ping operation from T-PE1 to T-PE2, enter the following command. *destination-address* is S-PE1 and *vc-id* is the VC between T-PE1 and S-PE1.

**ping mpls pseudowire** *destination-address* *vc-id*

- To perform a ping operation from T-PE1 to segment 2, enter the following command. *destination-address* is S-PE1 and *vc-id* is the VC between T-PE1 and S-PE1.

**ping mpls pseudowire** *destination-address* *vc-id* **segment** 2

**Step 2** **trace mpls pseudowire** *destination-address* *vc-id* **segment** *segment-number* [*segment-number*]

Where:

- *destination-address* is the address of the next S-PE router from the origin of the trace.



- *vc-id* is the VC ID of the segment from which the **trace** command is issued.
- *segment-number* indicates the segment upon which the trace operation will act. If you enter two segment numbers, the traceroute operation will perform a trace on that range of routers.

The following examples use the topology shown in [Figure 2](#):

- To perform a trace operation from T-PE1 to segment 2 of the multisegment pseudowire, enter the following command. *destination-address* is S-PE1 and *vc-id* is the VC between T-PE1 and S-PE1.

**trace mpls pseudowire destination-address vc-id segment 2**

This example performs a trace from T-PE1 to S-PE2.

- To perform a trace operation on a range of segments, enter the following command. This example performs a trace from S-PE2 to T-PE2. *destination-address* is S-PE1 and *vc-id* is the VC between T-PE1 and S-PE1.

**trace mpls pseudowire destination-address vc-id segment 2 4**

The following commands perform trace operations on S-PE router 10.10.10.9, first on segment 1, then on segment 2.

Segment 1 trace:

```
Router# trace mpls pseudowire 10.10.10.9 220 segment 1
```

Tracing MS-PW segments within range [1-1] peer address 10.10.10.9 and timeout 2 seconds

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
L 1 10.10.9.9 0 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220
```

Segment 2 trace:

```
Router# trace mpls pseudowire 10.10.10.9 220 segment 2
```

Tracing MS-PW segments within range [1-2] peer address 10.10.10.9 and timeout 2 seconds

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
L 1 10.10.9.9 4 ms [Labels: 18 Exp: 0]
    local 10.10.10.22 remote 10.10.10.9 vc id 220
```

```
! 2 10.10.3.3 4 ms [Labels: 16 Exp: 0]
    local 10.10.10.9 remote 10.10.10.3 vc id 220
```

# Additional References

The following sections provide references related to the L2VPN multisegment pseudowires feature.

## Related Documents

| Related Topic      | Document Title                                                                                                                                                                                               |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS commands | <i>Cisco IOS Master Commands List, All Releases</i>                                                                                                                                                          |
| MPLS commands      | <i>Cisco IOS Multiprotocol Label Switching Command Reference</i>                                                                                                                                             |
| Layer 2 VPNS       | <ul style="list-style-type: none"> <li>• <i>Any Transport over MPLS</i></li> <li>• <i>L2VPN Pseudowire Switching</i></li> <li>• <i>MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV</i></li> </ul> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                                                                               |
|----------|-------------------------------------------------------------------------------------|
| RFC 4447 | <i>Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)</i> |
| RFC5085  | <i>Pseudowire Virtual Circuit Connectivity Verification (VCCV)</i>                  |
| RFC4379  | <i>Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures</i>           |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for L2VPN Multisegment Pseudowires

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for L2VPN Multisegment Pseudowires

| Feature Name                   | Releases    | Feature Information                                                                                                                                                                                                   |
|--------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2VPN Multisegment Pseudowires | 12.2(33)SRE | This feature enables you to configure two or more Layer 2 pseudowire segments that function as a single pseudowire. The feature spans multiple cores or autonomous systems of the same or different carrier networks. |

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



# QoS Policy Support for L2VPN ATM PVPs

---

**First Published: February 27, 2009**

**Last Updated: November 20, 2009**

This document explains how to configure Quality of Service (QoS) Policy Support for Layer 2 Virtual Private Network (L2VPN) ATM permanent virtual paths (PVPs). That is, it explains how to configure QoS policies in ATM PVP mode for L2VPNs.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for QoS Policy Support for L2VPN ATM PVPs”](#) section on page 10.

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

## Contents

- [Prerequisites for QoS Policy Support for L2VPN ATM PVPs, page 2](#)
- [Restrictions for QoS Policy Support for L2VPN ATM PVPs, page 2](#)
- [Information About QoS Policy Support for L2VPN ATM PVPs, page 2](#)
- [How to Configure QoS Policy Support for L2VPN ATM PVPs, page 3](#)
- [Configuration Examples for QoS Policy Support for L2VPN ATM PVPs, page 7](#)
- [Additional References, page 8](#)
- [Feature Information for QoS Policy Support for L2VPN ATM PVPs, page 10](#)



---

**Americas Headquarters:**

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

© 2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for QoS Policy Support for L2VPN ATM PVPs

Before configuring QoS policies on L2VPN ATM PVPs, you should understand the concepts and configuration instructions in the following document:

- [Any Transport over MPLS](#)

## Restrictions for QoS Policy Support for L2VPN ATM PVPs

The following restrictions apply to the QoS Policy Support for L2VPN ATM PVPs feature:

- The Cisco 7600 series router does not support any queueing features in ATM PVP mode.
- When you enable a policy in PVP mode, do not configure ATM rates on the VCs that are part of the PVP. The VCs should be unspecified bit rate (UBR) VCs only.
- If VCs are part of a PVP that has a policy configured, you cannot configure ATM VC traffic shaping.
- Cisco IOS Release 12.2(33)SRE does not support cell-based ATM shaping per PVP.
- You cannot configure a queueing policy on an ATM PVP with UBR.
- You cannot configure queueing-based policies with UBR traffic shaping.

## Information About QoS Policy Support for L2VPN ATM PVPs

Before configuring the QoS Policy Support for L2VPN ATM PVPs feature, you should understand the following concepts:

- [MQC Structure, page 2](#)
- [Elements of a Traffic Class, page 3](#)
- [Elements of a Traffic Policy, page 3](#)

## MQC Structure

The modular QoS command-line interface (CLI) (MQC) structure allows you to define a traffic class, create a traffic policy, and attach the traffic policy to an interface.

The MQC structure is the result of the following three high-level steps.

1. Define a traffic class by using the **class-map** command. A traffic class is used to classify traffic.
2. Create a traffic policy by using the **policy-map** command. (The terms traffic policy and policy map are often synonymous.) A traffic policy (policy map) contains a traffic class and one or more QoS features that will be applied to the traffic class. The QoS features in the traffic policy determine how to treat the classified traffic.
3. Attach the traffic policy (policy map) to the interface by using the **service-policy** command.

## Elements of a Traffic Class

A traffic class contains three major elements: a traffic class name, a series of match commands, and, if more than one match command is used in the traffic class, instructions on how to evaluate these match commands.

The match commands are used for classifying packets. Packets are checked to determine whether they meet the criteria specified in the match commands; if a packet meets the specified criteria, that packet is considered a member of the class. Packets that fail to meet the matching criteria are classified as members of the default traffic class.

## Elements of a Traffic Policy

A traffic policy contains three elements: a traffic policy name, a traffic class (specified with the **class** command), and the command used to enable the QoS feature.

The traffic policy (policy map) applies the enabled QoS feature to the traffic class once you attach the policy map to the interface (by using the **service-policy** command).

**Note**

A packet can match only one traffic class within a traffic policy. If a packet matches more than one traffic class in the traffic policy, the first traffic class defined in the policy will be used.

## How to Configure QoS Policy Support for L2VPN ATM PVPs

The following sections explain how to configure QoS operations in ATM PVP mode:

- [Enabling a Service Policy in ATM PVP Mode, page 3](#) (required)
- [Enabling Traffic Shaping in ATM PVP Mode, page 5](#) (required)
- [Enabling Matching of ATM VCIs, page 6](#) (required)

## Enabling a Service Policy in ATM PVP Mode

You can enable a service policy in ATM PVP mode. You can also enable a service policy on PVP on a multipoint subinterface.

### Restrictions

- The Cisco 7600 series router does not support a service policy that uses the **match atm-vci** command in the egress direction.
- The **show policy-map interface** command does not display service policy information for ATM interfaces.
- Cisco IOS Release 12.2(33)SRE does not support cell-based ATM shaping per PVP.

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface atm *slot/port***
4. **atm pvp *vpi* l2transport**
5. **service-policy [input | output] *policy-map-name***
6. **xconnect *peer-router-id* *vcid* encapsulation mpls**
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                            |
| Step 3 | <b>interface atm <i>slot/port</i></b><br><br><b>Example:</b><br>Router(config)# interface atm 1/0                                                                          | Defines the interface and enters interface configuration mode.                                                                                                                                                                                                                                               |
| Step 4 | <b>atm pvp <i>vpi</i> l2transport</b><br><br><b>Example:</b><br>Router(config-if)# atm pvp 1 l2transport                                                                   | Specifies that the PVP is dedicated to transporting ATM cells and enters l2transport PVP configuration mode. <ul style="list-style-type: none"> <li>The <b>l2transport</b> keyword indicates that the PVP is for cell relay. This mode is for Layer 2 transport only; it is not for regular PVPs.</li> </ul> |
| Step 5 | <b>service-policy [input   output] <i>policy-map-name</i></b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvp)# service policy input poll                       | Enables a service policy on the specified PVP.                                                                                                                                                                                                                                                               |
| Step 6 | <b>xconnect <i>peer-router-id</i> <i>vcid</i> encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls | Binds the attachment circuit to a pseudowire VC. <ul style="list-style-type: none"> <li>The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                                                                                                                              |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-if-atm-l2trans-pvp)# end                                                                                                | Exits l2transport PVP configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                |



## Enabling Traffic Shaping in ATM PVP Mode

Traffic shaping commands are supported in ATM PVP mode. For egress VP shaping, one configuration command is supported for each ATM service category. The supported service categories are constant bit rate (CBR), UBR, variable bit rate-nonreal time (VBR-NRT), and variable bit rate real-time (VBR-RT).

### Restrictions

- The Cisco 7600 series router does not support traffic shaping.
- Cisco IOS Release 12.2(33)SRE does not support cell-based ATM shaping per PVP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface atm *slot/port***
4. **atm pvp *vpi* l2transport**
5. **ubr *pcr***  
or  
**cbr *pcr***  
or  
**vbr-nrt *pcr scr mbs***  
or  
**vbr-rt *pcr scr mbs***
6. **xconnect *peer-router-id vcid* encapsulation mpls**

### DETAILED STEPS

|        | Command or Action                                                                                        | Purpose                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                   | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>interface atm <i>slot/port</i></b><br><br><b>Example:</b><br>Router(config)# interface atm 1/0        | Defines the interface and enters interface configuration mode.                                                                                                                                                                                                                                                     |
| Step 4 | <b>atm pvp <i>vpi</i> l2transport</b><br><br><b>Example:</b><br>Router(config-if)# atm pvp 1 l2transport | Specifies that the PVP is dedicated to transporting ATM cells, and enters l2transport PVP configuration mode.<br><ul style="list-style-type: none"> <li>• The <b>l2transport</b> keyword indicates that the PVP is for cell relay. This mode is for Layer 2 transport only; it is not for regular PVPs.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>ubr pcr or cbr pcr or vbr-nrt pcr scr mbs or vbr-rt pcr scr mbs</pre> <p><b>Example:</b><br/> Router(config-if-atm-l2trans-pvp)# cbr 1000<br/> or<br/> cbr 56<br/> or<br/> vbr-nrt 11760 11760 1<br/> or<br/> vbr-rt 640 320 80</p> | <p>Enables traffic shaping in ATM PVP mode.</p> <ul style="list-style-type: none"> <li>• <i>pcr</i> = peak cell rate</li> <li>• <i>scr</i> = sustain cell rate</li> <li>• <i>mbs</i> = maximum burst size</li> </ul> |
| Step 6 | <pre>xconnect peer-router-id vcid encapsulation mpls</pre> <p><b>Example:</b><br/> Router(config-if-atm-l2trans-pvp)# xconnect 10.0.0.1 123 encapsulation mpls</p>                                                                       | <p>Binds the attachment circuit to a pseudowire VC.</p> <ul style="list-style-type: none"> <li>• The syntax for this command is the same as for all other Layer 2 transports.</li> </ul>                             |

## Enabling Matching of ATM VCIs

You can enable packet matching on an ATM VCI or range of VCIs using the **match atm-vci** command in class map configuration mode.

### Restrictions

- When you configure the **match atm-vci** command in class map configuration mode, you can add this class map to a policy map that can be attached only to an ATM VP.
- On the Cisco 7600 series router, the **match atm-vci** command is supported only in the ingress direction on an ATM VP.
- Cisco IOS Release 12.2(33)SRE does not support cell-based ATM shaping per PVP.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all** | **match-any**]
4. **match atm-vci** *vc-id* [*-vc-id*]
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                         | Purpose                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                                                                                                                                                 |
| Step 3 | <b>class-map</b> <i>class-map-name</i> [ <b>match-all</b>   <b>match-any</b> ]<br><br><b>Example:</b><br>Router(config)# class-map class1 | Creates a class map to be used for matching traffic to a specified class, and enters class map configuration mode.                                                                                                                                |
| Step 4 | <b>match atm-vci</b> <i>vc-id</i> [- <i>vc-id</i> ]<br><br><b>Example:</b><br>Router(config-cmap)# match atm-vci 50                       | Enables packet matching on an ATM VCI or range of VCIs. <ul style="list-style-type: none"> <li>The range is 32 to 65535.</li> </ul> <b>Note</b> You can use the <b>match not</b> command to match any VC except those you specify in the command. |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-cmap)# end                                                                             | (Optional) Returns to privileged EXEC mode.                                                                                                                                                                                                       |

## Configuration Examples for QoS Policy Support for L2VPN ATM PVPs

The following section shows an example of the QoS Policy Support for L2VPN ATM PVPs feature:

- [Enabling Traffic Shaping in ATM PVP Mode: Example, page 7](#)

### Enabling Traffic Shaping in ATM PVP Mode: Example

The following example enables traffic shaping in ATM PMP mode.

```
interface atm 1/0
 atm pvp 100 l2transport
 ubr 1000
 xconnect 10.11.11.11 777 encapsulation mpls
 atm pvp 101 l2transport
 ubr 1000
 xconnect 10.11.11.11 888 encapsulation mpls
 atm pvp 102 l2transport
 vbr-nrt 1200 800 128
 xconnect 10.11.11.11 999 encapsulation mpls
```

# Additional References

The following sections provide references related to the QoS Policy Support for L2VPN ATM PVPs feature.

## Related Documents

| Related Topic           | Document Title                                                            |
|-------------------------|---------------------------------------------------------------------------|
| Cisco IOS commands      | <a href="#">Cisco IOS Master Commands List, All Releases</a>              |
| MPLS commands           | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |
| Any Transport over MPLS | <a href="#">Any Transport over MPLS</a>                                   |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                                                    | MIBs Link                                                                                                                                                                                                                         |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>None</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |

# Feature Information for QoS Policy Support for L2VPN ATM PVPs

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for QoS Policy Support for L2VPN ATM PVPs

| Feature Name                          | Releases    | Feature Information                                                                                                                                                                                                                                                  |
|---------------------------------------|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| QoS Policy Support for L2VPN ATM PVPs | 12.2(33)SRE | <p>This feature enables you to configure QoS policies in ATM PVP mode for L2VPNs.</p> <p>The following commands were introduced or modified by this feature: <b>cbr</b>, <b>match atm-vci</b>, <b>service-policy</b>, <b>ubr</b>, <b>vbr-nrt</b>, <b>vbr-rt</b>.</p> |

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



# L2VPN: Pseudowire Preferential Forwarding

---

**First Published: February 27, 2009**

**Last Updated: November 20, 2009**

The L2VPN: Pseudowire Preferential Forwarding feature allows you to configure pseudowires so that you can use **ping**, **show**, and **traceroute** commands to find status information of the pseudowires before, during, and after a switchover.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for L2VPN: Pseudowire Preferential Forwarding](#)” section on [page 9](#).

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

## Contents

- [Prerequisites for L2VPN: Pseudowire Preferential Forwarding, page 2](#)
- [Restrictions for L2VPN: Pseudowire Preferential Forwarding, page 2](#)
- [Information About L2VPN: Pseudowire Preferential Forwarding, page 2](#)
- [How to Configure L2VPN: Pseudowire Preferential Forwarding, page 3](#)
- [Configuration Examples for L2VPN: Pseudowire Preferential Forwarding, page 5](#)
- [Additional References, page 7](#)
- [Feature Information for L2VPN: Pseudowire Preferential Forwarding, page 9](#)



---

**Americas Headquarters:**

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

© 2009 Cisco Systems, Inc. All rights reserved.

## Prerequisites for L2VPN: Pseudowire Preferential Forwarding

- Before configuring the L2VPN: Pseudowire Preferential Forwarding feature, you should understand the concepts in the following documents:
  - [Preferential Forwarding Status Bit Definition](#) (draft-ietf-pwe3-redundancy-bit-xx.txt)
  - [MPLS Pseudowire Status Signaling](#)
  - [L2VPN Pseudowire Redundancy](#)
  - [NSF/SSO—Any Transport over MPLS and AToM Graceful Restart](#)
  - [MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV](#)
- The provider edge (PE) routers must be configured with the following features:
  - L2VPN Pseudowire Redundancy
  - NSF/SSO—AToM and AToM Graceful Restart
- The L2VPN: Pseudowire Preferential Forwarding feature requires that the following mechanisms be in place to enable you to detect a failure in the network:
  - LSP Ping/Traceroute and Any Transport over MPLS Virtual Circuit Connection Verification (AToM VCCV)
  - Local Management Interface (LMI)
  - Operation, Administration, and Maintenance (OAM)

## Restrictions for L2VPN: Pseudowire Preferential Forwarding

- Only ATM attachment circuits are supported.
- The following features are not supported:
  - Port mode cell relay
  - Any Transport over MPLS: AAL5 over MPLS
  - VC cell packing
  - OAM emulation
  - Integrated LMI/permanent virtual circuit (PVC)-D
  - PVC Range
  - L2TPv3 Pseudowire Redundancy
  - Local switching
  - Multiple backup pseudowires
  - Static pseudowires

## Information About L2VPN: Pseudowire Preferential Forwarding

The following section provides information about the L2VPN: Pseudowire Preferential Forwarding feature:

- [Overview of L2VPN: Pseudowire Preferential Forwarding, page 3](#)



## Overview of L2VPN: Pseudowire Preferential Forwarding

The L2VPN: Pseudowire Preferential Forwarding feature allows you to configure pseudowires so that you can use **ping**, **show**, and **traceroute** commands to find status information before, during, and after a switchover. The implementation of this feature is based on [Preferential Forwarding Status Bit Definition](#) (draft-ietf-pwe3-redundancy-bit-xx.txt). The L2VPN: Pseudowire Preferential Forwarding feature provides these enhancements for displaying information about the pseudowires:

- You can issue **ping mpls** commands on the backup pseudowires.
- You can display status of the pseudowires before, during, and after a switchover, using the **show xconnect** and **show mpls l2transport vc** commands.

**Note**

In a single-segment pseudowire, the PE routers at each end of the pseudowire serve as the termination points. In multisegment pseudowires, the terminating PE routers serve as the termination points.

## How to Configure L2VPN: Pseudowire Preferential Forwarding

The following section explains how to configure the L2VPN: Pseudowire Preferential Forwarding feature:

- [Configuring the Pseudowire, page 3](#) (required)

## Configuring the Pseudowire

You configure a connection, called a pseudowire, between the routers to transmit Layer 2 frames between PE routers.

As part of the pseudowire configuration, issue the **status redundancy master** command to make it the master. This enables the L2VPN: Pseudowire Preferential Forwarding feature to display the status of the active and backup pseudowires. By default, the PE router is in slave mode.

**Note**

One pseudowire must be the master and the other must be assigned the slave. You cannot configure both pseudowires as master or slave.

**Note**

You must specify the **encapsulation mpls** command as part of the pseudowire class for the Any Transport over MPLS (AToM) VCs to work properly. If you omit the **encapsulation mpls** command, you receive the following error:

```
% Incomplete command.
```

## Prerequisites

The PE routers must be configured for the L2VPN Pseudowire Redundancy and NSF/SSO—Any Transport over MPLS and AToM Graceful Restart features. See the following documents for configuration instructions:

- [L2VPN Pseudowire Redundancy](#)

- *NSF/SSO—Any Transport over MPLS and AToM Graceful Restart*

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**
5. **status redundancy** {**master** | **slave**}
6. **interworking** {**ethernet** | **ip**}

## DETAILED STEPS

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>pseudowire-class</b> <i>name</i><br><br><b>Example:</b><br>Router(config)# pseudowire-class atom                             | Establishes a pseudowire class with a name that you specify, and enters pseudowire class configuration mode.                                                                                                                                                                                                                                                                                                                                 |
| Step 4 | <b>encapsulation mpls</b><br><br><b>Example:</b><br>Router(config-pw)# encapsulation mpls                                       | Specifies the tunneling encapsulation.<br><ul style="list-style-type: none"><li>• For AToM, the encapsulation type is <b>mpls</b>.</li></ul>                                                                                                                                                                                                                                                                                                 |
| Step 5 | <b>status redundancy</b> { <b>master</b>   <b>slave</b> }<br><br><b>Example:</b><br>Router(config-pw)# status redundancy master | Specifies the pseudowire as the master or slave.<br><ul style="list-style-type: none"><li>• This enables the L2VPN: Pseudowire Preferential Forwarding feature to display the status of the active and backup pseudowires.</li><li>• By default, the PE router is in slave mode.</li></ul> <b>Note</b> One pseudowire must be the master and the other must be assigned the slave. You cannot configure both pseudowires as master or slave. |
| Step 6 | <b>interworking</b> { <b>ethernet</b>   <b>ip</b> }<br><br><b>Example:</b><br>Router(config-pw)# interworking ip                | (Optional) Enables the translation between the different Layer 2 encapsulations.                                                                                                                                                                                                                                                                                                                                                             |

# Configuration Examples for L2VPN: Pseudowire Preferential Forwarding

This section contains the following examples:

- [L2VPN: Pseudowire Preferential Forwarding Configuration: Example, page 5](#)
- [Displaying the Status of the Pseudowires: Example, page 5](#)

## L2VPN: Pseudowire Preferential Forwarding Configuration: Example

The following commands configure a PE router with the L2VPN: Pseudowire Preferential Forwarding feature:

```
mpls ldp graceful-restart
mpls ip
mpls label protocol ldp
mpls ldp router-id Loopback0 force
mpls ldp advertise-labels
!
pseudowire-class mpls
  encapsulation mpls
  status redundancy master

interface ATM0/2/0.1 multipoint
  logging event subif-link-status
  atm pvp 50 l2transport
  xconnect 10.1.1.2 100 encap mpls
  backup peer 10.1.1.3 100 encap mpls
end
```

## Displaying the Status of the Pseudowires: Example

The following examples show the status of the active and backup pseudowires before, during, and after a switchover.

The **show mpls l2transport vc** command on the active PE router displays the status of the pseudowires:

Router# **show mpls l2transport vc**

| Local intf | Local circuit   | Dest address | VC ID | Status  |
|------------|-----------------|--------------|-------|---------|
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.2     | 100   | UP      |
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.3     | 100   | STANDBY |

The **show mpls l2transport vc** command on the backup PE router displays the status of the pseudowires. The active pseudowire on the backup PE router has the HOTSTANDBY status.

Router-standby# **show mpls l2transport vc**

| Local intf | Local circuit   | Dest address | VC ID | Status     |
|------------|-----------------|--------------|-------|------------|
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.2     | 100   | HOTSTANDBY |
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.3     | 100   | DOWN       |

During a switchover, the status of the active and backup pseudowires changes:

| Local intf | Local circuit   | Dest address | VC ID | Status     |
|------------|-----------------|--------------|-------|------------|
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.2     | 100   | RECOVERING |
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.3     | 100   | DOWN       |

| Local intf | Local circuit   | Dest address | VC ID | Status  |
|------------|-----------------|--------------|-------|---------|
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.2     | 100   | UP      |
| AT0/2/0.1  | ATM VPC CELL 50 | 10.1.1.3     | 100   | STANDBY |

```

-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
UP pri ac  AT1/1/0.1/1/1:220/220(ATM V  UP mpls 10.193.193.3:330      UP
IA sec ac  AT1/1/0.1/1/1:220/220(ATM V  UP mpls 10.193.193.3:331      SB

```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
! 1 10.193.33.22 4 ms [Labels: 23 Exp: 0]
    local 10.193.193.3 remote 10.193.193.22 vc id 331
```

## Additional References

The following sections provide references related to the L2VPN: Pseudowire Preferential Forwarding feature.

## Related Documents

| Related Topic                  | Document Title                                                                                                                                              |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco IOS commands             | <a href="#">Cisco IOS Master Commands List, All Releases</a>                                                                                                |
| MPLS commands                  | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>                                                                                   |
| L2VPN pseudowires              | <ul style="list-style-type: none"> <li>• <a href="#">MPLS Pseudowire Status Signaling</a></li> <li>• <a href="#">L2VPN Pseudowire Redundancy</a></li> </ul> |
| NSF/SSO for L2VPNs             | <a href="#">NSF/SSO—Any Transport over MPLS and AToM Graceful Restart</a>                                                                                   |
| Ping and traceroute for L2VPNs | <a href="#">MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV</a>                                                                                  |

## Standards

| Standard                              | Title                                                         |
|---------------------------------------|---------------------------------------------------------------|
| draft-ietf-pwe3-redundancy-bit-xx.txt | <a href="#">Preferential Forwarding Status Bit Definition</a> |

## MIBs

| MIB                                                     | MIBs Link                                                                                                                                                                                                                         |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• N/A</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# Feature Information for L2VPN: Pseudowire Preferential Forwarding

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for L2VPN: Pseudowire Preferential Forwarding

| Feature Name                              | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| L2VPN: Pseudowire Preferential Forwarding | 12.2(33)SRE | <p>This feature allows you to configure pseudowires so that you can use <b>ping</b>, <b>show</b>, and <b>tracert</b> commands to find status information of the pseudowires before, during, and after a switchover.</p> <p>The following commands were introduced or modified by this feature: <b>show mpls l2transport vc</b>, <b>show xconnect</b>, <b>status redundancy</b>.</p> |

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



## **MPLS Layer 3 VPNs**







# Configuring MPLS Layer 3 VPNs

---

**First Published: May 2, 2005**

**Last Updated: August 26, 2008**

A Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers. This module explains how to create an MPLS VPN.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Layer 3 VPNs” section on page 37](#).

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

## Contents

- [Prerequisites for MPLS Layer 3 VPNs, page 2](#)
- [Restrictions for MPLS Layer 3 VPNs, page 2](#)
- [Information about MPLS Layer 3 VPNs](#)
- [How to Configure MPLS Layer 3 VPNs](#)
- [Configuration Examples for MPLS VPNs, page 29](#)
- [Additional References, page 35](#)
- [Feature Information for MPLS Layer 3 VPNs, page 37](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS Layer 3 VPNs

Before configuring MPLS Layer 3 VPNs, you should have MPLS, Label Distribution Protocol (LDP), and Cisco Express Forwarding (CEF) installed in your network. All routers in the core, including the PE routers, must be able to support CEF and MPLS forwarding. See [“Assessing the Needs of MPLS VPN Customers” section on page 9](#) for more information.

## Restrictions for MPLS Layer 3 VPNs

When configuring static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.xT, 12.xM, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later. Use the following guidelines when configuring static routes.

### Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in MPLS environment:

```
ip route destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

```
ip route destination-prefix mask interface1 next-hop1  
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the next hop can be reached through two paths:

```
ip route destination-prefix mask next-hop-address
```

The following **ip route** command is not supported when you configure static routes in an MPLS environment and enable load sharing where the destination can be reached through two next hops:

```
ip route destination-prefix mask next-hop1  
ip route destination-prefix mask next-hop2
```

Use the *interface* and *next-hop* arguments when specifying static routes.

### Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop and interface are in the same VRF:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask* **interface1 next-hop1**  
**ip route vrf** *vrf-name destination-prefix mask* **interface2 next-hop2**

The following **ip route vrf** commands are supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the Internet Gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address* **global**
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and interface are in the core.)

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS VPN Environment that Uses the TFIB

The following **ip route** command is not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in a MPLS VPN environment, and the next hop is in the global table on the CE side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in a MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static non-recursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

# Information about MPLS Layer 3 VPNs

Before configuring MPLS Layer 3 VPNs, you should understand the following concepts:

- [MPLS VPN Definition, page 4](#)
- [How an MPLS VPN Works, page 5](#)
- [Major Components of MPLS VPNs, page 7](#)
- [Benefits of an MPLS VPN, page 7](#)

## MPLS VPN Definition

Before defining an MPLS VPN, you need to define a VPN in general. A VPN is:

- An IP-based network delivering private network services over a public infrastructure
- A set of sites that are allowed to communicate with each other privately over the Internet or other public or private networks

Conventional VPNs are created by configuring a full mesh of tunnels or permanent virtual circuits (PVCs) to all sites in a VPN. This type of VPN is not easy to maintain or expand, because adding a new site requires changing each edge device in the VPN.

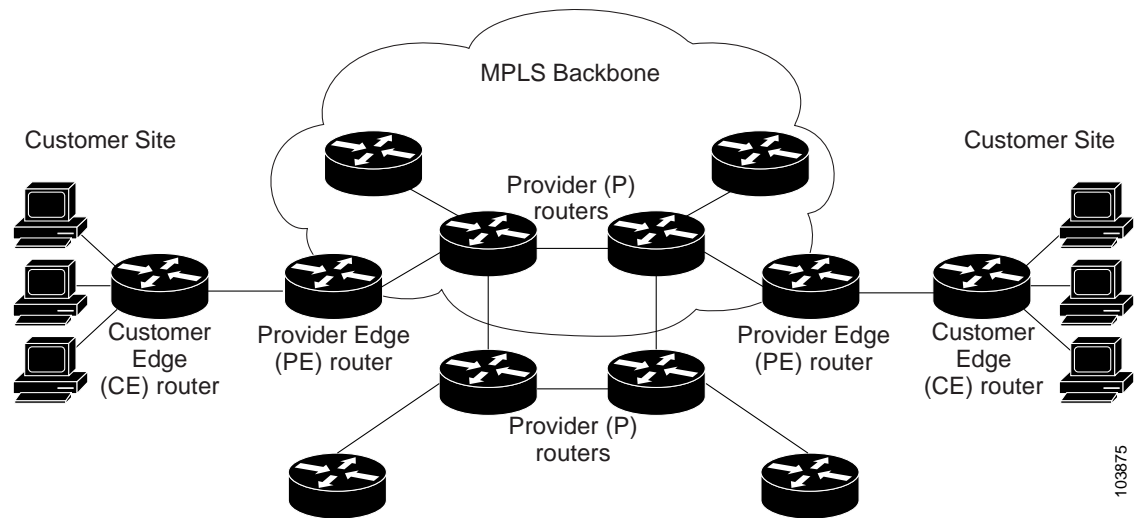
MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without the customer's involvement.

MPLS VPNs are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS VPN, only the service provider's edge router that provides services to the customer site needs to be updated.

The different parts of the MPLS VPN are described as follows:

- **Provider (P) router**—Router in the core of the provider network. P routers run MPLS switching, and do not attach VPN labels (MPLS label in each route assigned by the PE router) to routed packets. VPN labels are used to direct data packets to the correct egress router.
- **PE router**—Router that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received. A PE router attaches directly to a CE router.
- **Customer (C) router**—Router in the ISP or enterprise network.
- **Customer edge router**—Edge router on the network of the ISP that connects to the PE router on the network. A CE router must interface with a PE router.

[Figure 1](#) shows a basic MPLS VPN.

**Figure 1 Basic MPLS VPN Terminology**

103875

## How an MPLS VPN Works

MPLS VPN functionality is enabled at the edge of an MPLS network. The PE router performs the following:

- Exchanges routing updates with the CE router
- Translates the CE routing information into VPNv4 routes
- Exchanges VPNv4 routes with other PE routers through the Multiprotocol Border Gateway Protocol (MP-BGP)

## How Virtual Routing/Forwarding Tables Work in an MPLS VPN

Each VPN is associated with one or more virtual routing and forwarding (VRF) instances. A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of the following components:

- An IP routing table
- A derived CEF table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters that control the information that is included in the routing table

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A site can be a member of multiple VPNs. However, a site can associate with only one VRF. A site's VRF contains all the routes available to the site from the VPNs of which it is a member.

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

## How VPN Routing Information Is Distributed in an MPLS VPN

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

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

## BGP Distribution of VPN Routing Information

A PE router can learn an IP prefix from the following sources:

- A CE router by static configuration
- A BGP session with the CE router
- A Routing Information Protocol (RIP) exchange with the CE router

The IP prefix is a member of the IPv4 address family. After the PE router learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses. The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the VRF on the PE router.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels:

- Within IP domains, known as an autonomous system (interior BGP [IBGP])
- Between autonomous systems (external BGP [EBGP]).

PE-PE or PE-RR (route reflector) sessions are IBGP sessions, and PE-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (refer to RFC 2283, *Multiprotocol Extensions for BGP-4*), which define support for address families other than IPv4. Using the extensions ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

## MPLS Forwarding

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

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network reachability information for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet,

it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

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

## Major Components of MPLS VPNs

An MPLS-based VPN network has three major components:

- **VPN route target communities**—A VPN route target community is a list of all members of a VPN community. VPN route targets need to be configured for each VPN community member.
- **Multiprotocol BGP (MP-BGP) peering of VPN community PE routers**—MP-BGP propagates VRF reachability information to all members of a VPN community. MP-BGP peering needs to be configured in all PE routers within a VPN community.
- **MPLS forwarding**—MPLS transports all traffic between all VPN community members across a VPN service-provider network.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can associate with only one VRF. A customer-site VRF contains all the routes available to the site from the VPNs of which it is a member.

## Benefits of an MPLS VPN

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

**Connectionless Service**—A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, a VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. When you create a connectionless VPN, you do not need tunnels and encryption for network privacy, thus eliminating significant complexity.

**Centralized Service**—Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services. It must also provide a way to flexibly deliver value-added services to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS VPNs are seen as private intranets, you may use new IP services such as:

- Multicast
- Quality of service (QoS)
- Telephony support within a VPN
- Centralized services including content and web hosting to a VPN



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

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

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

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

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

**Security**—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

Security is provided in the following areas:

- At the edge of a provider network, ensuring packets received from a customer are placed on the correct VPN.
- At the backbone, VPN traffic is kept separate. Malicious spoofing (an attempt to gain access to a PE router) is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

**Easy to Create**—To take full advantage of VPNs, customers must be able to easily create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. You can add sites to intranets and extranets and form closed user groups. Managing VPNs in this manner enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.

**Flexible Addressing**—To make a VPN service more accessible, customers of a service provider can design their own addressing plan, independent of addressing plans for other service provider customers. Many customers use private address spaces, as defined in RFC 1918, and do not want to invest the time and expense of converting to public IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without network address translation (NAT) by providing a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate. This enables customers to use their own unregistered private addresses, and communicate freely across a public IP network.

**Integrated Quality of Service (QoS) Support**—QoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:

- Predictable performance and policy implementation
- Support for multiple levels of service in an MPLS VPN

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

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

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

## How to Configure MPLS Layer 3 VPNs

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

- [Configuring the Core Network, page 9](#) (required)
- [Connecting the MPLS VPN Customers, page 13](#) (required)
- [Verifying Connectivity Between MPLS VPN Sites, page 27](#) (optional)

### Configuring the Core Network

Configuring the core network includes the following tasks:

- [Assessing the Needs of MPLS VPN Customers, page 9](#) (required)
- [Configuring Routing Protocols in the Core, page 10](#) (required)
- [Configuring MPLS in the Core, page 10](#) (required)
- [Determining if CEF Is Enabled in the Core, page 10](#) (required)
- [Configuring Multiprotocol BGP on the PE Routers and Route Reflectors, page 11](#) (required)

### Assessing the Needs of MPLS VPN Customers

Before you configure an MPLS VPN, you need to identify the core network topology so that it can best serve MPLS VPN customers. Perform this task to identify the core network topology.

#### SUMMARY STEPS

1. Identify the size of the network.
2. Identify the routing protocols.
3. Determine if you need MPLS High Availability support.
4. Determine if you need BGP load sharing and redundant paths.

## DETAILED STEPS

|               | Command or Action                                                                | Purpose                                                                                                                                                                                                                                                                                                       |
|---------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Identify the size of the network.                                                | Identify the following to determine the number of routers and ports you need: <ul style="list-style-type: none"> <li>How many customers do you need to support?</li> <li>How many VPNs are needed per customer?</li> <li>How many virtual routing and forwarding instances are there for each VPN?</li> </ul> |
| <b>Step 2</b> | Identify the routing protocols in the core.                                      | Determine which routing protocols you need in the core network.                                                                                                                                                                                                                                               |
| <b>Step 3</b> | Determine if you need MPLS VPN High Availability support.                        | MPLS VPN Nonstop Forwarding and Graceful Restart are supported on select routers and Cisco IOS releases. Contact Cisco Support for the exact requirements and hardware support.                                                                                                                               |
| <b>Step 4</b> | Determine if you need BGP load sharing and redundant paths in the MPLS VPN core. | See <a href="#">Load Sharing MPLS VPN Traffic</a> for configuration steps.                                                                                                                                                                                                                                    |

## Configuring Routing Protocols in the Core

To configure a routing protocol—BGP, OSPF, IS-IS, EIGRP, static—see [Configuring IP Routing Protocols](#).

## Configuring MPLS in the Core

To enable MPLS on all routers in the core, you must configure a label distribution protocol. You can use either of the following as a label distribution protocol:

- MPLS Label Distribution Protocol (LDP). For configuration information, see the [Configuring MPLS Label Distribution Protocol \(LDP\)](#).
- MPLS Traffic Engineering Resource Reservation Protocol (RSVP). For configuration information, see [Configuring MPLS Traffic Engineering](#).

## Determining if CEF Is Enabled in the Core

Cisco Express Forwarding (CEF) must be enabled all routers in the core, including the PE routers. For information about how to determine if CEF is enabled, see [Configuring Basic Cisco Express Forwarding—Improving Performance, Scalability, and Resiliency in Dynamic Network](#).

## Configuring Multiprotocol BGP on the PE Routers and Route Reflectors

Perform this task to configure multiprotocol BGP (MP-BGP) connectivity on the PE routers and route reflectors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **address-family vpv4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                  | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                     | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast | (Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>Use the <b>no</b> form of the <b>bgp default ipv4-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                                                       |

|                | Command or Action                                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b>  | <pre>neighbor {ip-address   peer-group-name} remote-as as-number</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor pp.0.0.1<br/>remote-as 100</p>                  | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| <b>Step 6</b>  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router)# neighbor pp.0.0.1<br/>activate</p>                                  | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| <b>Step 7</b>  | <pre>address-family vpnv4 [unicast]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family vpnv4</p>                                                              | <p>Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.</p> <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                   |
| <b>Step 8</b>  | <pre>neighbor {ip-address   peer-group-name} send-community extended</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1<br/>send-community extended</p> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                               |
| <b>Step 9</b>  | <pre>neighbor {ip-address   peer-group-name} activate</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor pp.0.0.1<br/>activate</p>                               | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| <b>Step 10</b> | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                                       | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                           |

## Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Connecting the MPLS VPN Customers

To connect the MPLS VPN customers to the VPN, perform the following tasks:

- [Defining VRFs on the PE Routers to Enable Customer Connectivity, page 13](#) (required)
- [Configuring VRF Interfaces on PE Routers for Each VPN Customer, page 14](#) (required)
- [Configuring Routing Protocols Between the PE and CE Routers, page 15](#) (required)

### Defining VRFs on the PE Routers to Enable Customer Connectivity

To define VPN routing and forwarding (VRF) instances, perform this task.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd *route-distinguisher***
5. **route-target {import | export | both} *route-target-ext-community***
6. **import map *route-map***
7. **exit**

#### DETAILED STEPS

|        | Command or Action                              | Purpose                                                                                                         |
|--------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                  | Enables privileged EXEC mode.                                                                                   |
|        | <b>Example:</b><br>Router> enable              | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                            |
| Step 2 | <b>configure terminal</b>                      | Enters global configuration mode.                                                                               |
|        | <b>Example:</b><br>Router# configure terminal  |                                                                                                                 |
| Step 3 | <b>ip vrf <i>vrf-name</i></b>                  | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode.                     |
|        | <b>Example:</b><br>Router(config)# ip vrf vpn1 | <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul> |

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# <b>rd</b> 100:1                                                                                      | Creates routing and forwarding tables. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                                    |
| Step 5 | <b>route-target</b> { <b>import</b>   <b>export</b>   <b>both</b> }<br><i>route-target-ext-community</i><br><br><b>Example:</b><br>Router(config-vrf)# <b>route-target import</b> 100:1 | Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6 | <b>import map</b> <i>route-map</i><br><br><b>Example:</b><br>Router(config-vrf)# <b>import map</b> vpn1-route-map                                                                       | (Optional) Configures an import route map for a VRF. <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# <b>exit</b>                                                                                                                   | (Optional) Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring VRF Interfaces on PE Routers for Each VPN Customer

To associate a VRF with an interface or subinterface on the PE routers, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                               | Enters global configuration mode.                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 5/0         | Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                            |
| Step 5 | <b>end</b><br><br>Router(config-if)# end                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                               |

## Configuring Routing Protocols Between the PE and CE Routers

Configure the PE router with the same routing protocol that the CE router uses. You can configure the following routing protocols:

- [Configuring BGP as the Routing Protocol Between the PE and CE Routers, page 15](#)
- [Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers, page 17](#)
- [Configuring Static Routes Between the PE and CE Routers, page 19](#)
- [Configuring OSPF as the Routing Protocol Between the PE and CE Routers, page 21](#)
- [Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23](#)
- [Configuring EIGRP Redistribution in the MPLS VPN, page 25](#)

### Configuring BGP as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using BGP, perform this task.

## SUMMARY STEPS

- enable**
- configure terminal**
- router bgp** *as-number*



4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **exit-address-family**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                 | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                           |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1 | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1 remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor pp.0.0.1 activate                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 7 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                   | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                            |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                      | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                           |

## Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions using RIPv2, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router rip**
4. **version** {1 | 2}
5. **address-family** ipv4 [multicast | unicast | vrf *vrf-name*]
6. **network** *ip-address*
7. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>router rip</b><br><br><b>Example:</b><br>Router(config)# router rip                                                                                                                                                                                                                                   | Enables RIP.                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>version {1   2}</b><br><br><b>Example:</b><br>Router(config-router)# version 2                                                                                                                                                                                                                        | Specifies a Routing Information Protocol (RIP) version used globally by the router.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 5 | <b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1                                                                                                                                                            | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 6 | <b>network ip-address</b><br><br><b>Example:</b><br>Router(config-router-af)# network 192.168.7.0                                                                                                                                                                                                        | Enables RIP on the PE-to-CE link.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 7 | <b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b><br><br><b>Example:</b><br>Router(config-router-af)# redistribute bgp 200 | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>For the RIPv2 routing protocol, use the <b>redistribute bgp as-number</b> command.</li> </ul> See the <a href="#">redistribute</a> command for information about other arguments and keywords.                                                                                                                                               |

|        | Command or Action                                                                                  | Purpose                                   |
|--------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

## Configuring Static Routes Between the PE and CE Routers

To configure PE-to-CE routing sessions that use static routes, perform this task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route vrf** *vrf-name*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
6. **redistribute** *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*as-number*] [**metric** *metric-value*] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**]
7. **exit-address-family**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>ip route vrf vrf-name</b><br><br><b>Example:</b><br>Router(config)# ip route vrf 200                                                                                                                                                                                                                    | Defines static route parameters for every PE-to-CE session.                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 4 | <b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1                                                                                                                                                              | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specifies the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b><br><br><b>Example:</b><br>Router(config-router-af)# redistribute static    | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>To redistribute VRF static routes into the VRF BGP table, use the <b>redistribute static</b> command.</li> </ul> See the command for information about other arguments and keywords.                                                                                                                                                         |
| Step 6 | <b>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</b><br><br><b>Example:</b><br>Router(config-router-af)# redistribute connected | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>To redistribute directly connected networks into the VRF BGP table, use the <b>redistribute connected</b> command.</li> </ul> See the <b>redistribute</b> command for information about other arguments and keywords.                                                                                                                        |

|        | Command or Action                                                                                                     | Purpose                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 7 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# <code>exit-address-family</code> | Exits address family configuration mode.  |
| Step 8 | <code>end</code><br><br><b>Example:</b><br>Router(config-router)# <code>end</code>                                    | (Optional) Exits to privileged EXEC mode. |

## Configuring OSPF as the Routing Protocol Between the PE and CE Routers

To configure PE-to-CE routing sessions that use OSPF, perform this task.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router ospf process-id [vrf vpn-name]`
4. `network ip-address wildcard-mask area area-id`
5. `address-family ipv4 [multicast | unicast | vrf vrf-name]`
6. `redistribute protocol [process-id] {level-1 | level-1-2 | level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal | external 1 | external 2}] [tag tag-value] [route-map map-tag] [subnets]`
7. `exit-address-family`
8. `end`

### DETAILED STEPS

|        | Command or Action                                                                                 | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> <code>enable</code>                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# <code>configure terminal</code> | Enters global configuration mode.                                                                                     |

|        | Command or Action                                                                                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>router ospf process-id [vrf vpn-name]</pre> <p><b>Example:</b><br/>Router(config)# router ospf 1 vrf grc</p>                                                                                                                                                                                                          | <p>Enables OSPF routing and enters router configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>process-id</i> argument identifies the OSPF process.</li> <li>The <b>vrf</b> keyword and <i>vpn-name</i> argument identify a VPN. Create a separate OSPF process for each VRF that will receive VPN routes.</li> </ul>                                                                                                                                                                                                                                                                                    |
| Step 4 | <pre>network ip-address wildcard-mask area area-id</pre> <p><b>Example:</b><br/>Router(config-router)# network 192.168.129.16 0.0.0.3 area 20</p>                                                                                                                                                                          | <p>Defines the interfaces on which OSPF runs and to defines the area ID for those interfaces.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument identifies the IP address.</li> <li>The <i>wildcard-mask</i> argument identifies the IP-address-type mask that includes “don't care” bits.</li> <li>The <i>area-id</i> argument identifies the area that is to be associated with the OSPF address range. It can be specified as either a decimal value or as an IP address. To associate areas with IP subnets, specify a subnet address as the value of the <i>area-id</i> argument.</li> </ul> |
| Step 5 | <pre>address-family ipv4 [multicast   unicast   vrf vrf-name]</pre> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf vpn1</p>                                                                                                                                                                         | <p>Specifies the IPv4 address family type and enters address family configuration mode.</p> <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                                                                 |
| Step 6 | <pre>redistribute protocol [process-id] {level-1   level-1-2   level-2} [as-number] [metric metric-value] [metric-type type-value] [match {internal   external 1   external 2}] [tag tag-value] [route-map map-tag] [subnets]</pre> <p><b>Example:</b><br/>Router(config-router-af)# redistribute rip metric 1 subnets</p> | <p>Redistributes routes from one routing domain into another routing domain.</p> <p>You may need to include several protocols to ensure that all IBGP routes are distributed into the VRF.</p> <p>See the <b>redistribute</b> command for information about other arguments and keywords.</p>                                                                                                                                                                                                                                                                                                                             |

|        | Command or Action                                                                                                     | Purpose                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 7 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# <code>exit-address-family</code> | Exits address family configuration mode.  |
| Step 8 | <code>end</code><br><br><b>Example:</b><br>Router(config-router)# <code>end</code>                                    | (Optional) Exits to privileged EXEC mode. |

### Configuring EIGRP as the Routing Protocol Between the PE and CE Routers

Using Enhanced Interior Gateway Routing Protocol (EIGRP) between the PE and CE routers allows you to transparently connect EIGRP customer networks through an MPLS-enabled BGP core network so that EIGRP routes are redistributed through the VPN across the BGP network as internal BGP (iBGP) routes.

To configure PE-to-CE routing sessions that use EIGRP, perform this task.

#### Prerequisites

BGP must be configured in the network core.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router bgp as-number`
4. `no synchronization`
5. `neighbor ip-address remote-as as-number`
6. `neighbor ip-address update-source loopback interface-number`
7. `address-family vpv4`
8. `neighbor ip-address activate`
9. `neighbor ip-address send-community extended`
10. `exit-address-family`
11. `address-family ipv4 vrf vrf-name`
12. `redistribute eigrp as-number [metric metric-value][route-map map-name]`
13. `no synchronization`
14. `exit-address-family`
15. `end`



## DETAILED STEPS

|        | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                       |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 10                                                                            | Enters router configuration mode, and creates a BGP routing process.                                                                                                                                                                                                    |
| Step 4 | <b>no synchronization</b><br><br><b>Example:</b><br>Router(config-router)# no synchronization                                                                  | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                                                                                                                      |
| Step 5 | <b>neighbor ip-address remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 remote-as 10                                 | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are establishing an iBGP session with the PE router that is connected to the CE router at the other CE site.</li> </ul>                         |
| Step 6 | <b>neighbor ip-address update-source loopback interface-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 update-source loopback 0 | Configures BGP to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>This configuration step is not required. However, the BGP routing process will be less susceptible to the affects of interface or link flapping.</li> </ul> |
| Step 7 | <b>address-family vpnv4</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                              | Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes, such as BGP, RIP, and static routing sessions.                                                                                                       |
| Step 8 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1 activate                                             | Establishes peering with the specified neighbor or peer-group. <ul style="list-style-type: none"> <li>In this step, you are activating the exchange of VPNv4 routing information between the PE routers.</li> </ul>                                                     |
| Step 9 | <b>neighbor ip-address send-community extended</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1 send-community extended               | Configures the local router to send extended community attribute information to the specified neighbor. <ul style="list-style-type: none"> <li>This step is required for the exchange of EIGRP extended community attributes.</li> </ul>                                |

|         | Command or Action                                                                                                                                              | Purpose                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                       | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                |
| Step 11 | <code>address-family ipv4 vrf vrf-name</code><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                     | Configures an IPv4 address-family for the EIGRP VRF and enters address family configuration mode. <ul style="list-style-type: none"> <li>An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE routers.</li> </ul> |
| Step 12 | <code>redistribute eigrp as-number [metric metric-value][route-map map-name]</code><br><br><b>Example:</b><br>Router(config-router-af)# redistribute eigrp 101 | Redistributes the EIGRP VRF into BGP. <ul style="list-style-type: none"> <li>The autonomous system number from the CE network is configured in this step.</li> </ul>                                                                                         |
| Step 13 | <code>no synchronization</code><br><br><b>Example:</b><br>Router(config-router-af)# no synchronization                                                         | Configures BGP to send advertisements without waiting to synchronize with the IGP.                                                                                                                                                                           |
| Step 14 | <code>exit-address-family</code><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                       | Exits address family configuration mode and enters router configuration mode.                                                                                                                                                                                |
| Step 15 | <code>end</code><br><br><b>Example:</b><br>Router(config-router)# end                                                                                          | Exits router configuration mode and enters privileged EXEC mode.                                                                                                                                                                                             |

## Configuring EIGRP Redistribution in the MPLS VPN

Perform this task to every PE router that provides VPN services to enable EIGRP redistribution in the MPLS VPN.

### Prerequisites

The metric must be configured for routes from external EIGRP autonomous systems and non-EIGRP networks before these routes can be redistributed into an EIGRP CE router. The metric can be configured in the redistribute statement using the **redistribute (IP)** command or configured with the **default-metric (EIGRP)** command. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE router.

### Restrictions

Redistribution between native EIGRP VRFs is not supported. This is designed behavior.

## SUMMARY STEPS

1. `enable`

2. **configure terminal**
3. **router eigrp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **network** *ip-address wildcard-mask*
6. **redistribute bgp** {*as-number*} [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map-name*]
7. **autonomous-system** *as-number*
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>router eigrp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router eigrp 1                                                                                                                                                       | Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> <li>The EIGRP routing process for the PE router is created in this step.</li> </ul>                                                                                                                                                                                  |
| Step 4 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf RED                                                                          | Enters address-family configuration mode and creates a VRF. <ul style="list-style-type: none"> <li>The VRF name must match the VRF name that was created in the previous section.</li> </ul>                                                                                                                                                                                   |
| Step 5 | <b>network</b> <i>ip-address wildcard-mask</i><br><br><b>Example:</b><br>Router(config-router-af)# network 172.16.0.0 0.0.255.255                                                                                                                   | Specifies the network for the VRF. <ul style="list-style-type: none"> <li>The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement.</li> </ul>                                                                                              |
| Step 6 | <b>redistribute bgp</b> { <i>as-number</i> } [ <b>metric</b> <i>bandwidth delay reliability load mtu</i> ] [ <b>route-map</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500 | Redistributes BGP into the EIGRP. <ul style="list-style-type: none"> <li>The autonomous system number and metric of the BGP network is configured in this step. BGP must be redistributed into EIGRP for the CE site to accept the BGP routes that carry the EIGRP information. A metric must also be specified for the BGP network and is configured in this step.</li> </ul> |

|        | Command or Action                                                                                                               | Purpose                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| Step 7 | <code>autonomous-system as-number</code><br><br><b>Example:</b><br><code>Router(config-router-af)# autonomous-system 101</code> | Specifies the autonomous system number of the EIGRP network for the customer site. |
| Step 8 | <code>exit-address-family</code><br><br><b>Example:</b><br><code>Router(config-router-af)# exit-address-family</code>           | Exits address family configuration mode and enters router configuration mode.      |
| Step 9 | <code>end</code><br><br><b>Example:</b><br><code>Router(config-router)# end</code>                                              | Exits router configuration mode and enters privileged EXEC mode.                   |

## Verifying the VPN Configuration

A route distinguisher must be configured for the VRF, and MPLS must be configured on the interfaces that carry the VRF. Use the **show ip vrf** command to verify the route distinguisher (RD) and interface that are configured for the VRF.

### SUMMARY STEPS

1. **show ip vrf**

### DETAILED STEPS

#### Step 1 **show ip vrf**

Use this command to display the set of defined VRF instances and associated interfaces. The output also maps the VRF instances to the configured route distinguisher.

## Verifying Connectivity Between MPLS VPN Sites

To verify that the local and remote CE routers can communicate across the MPLS core, perform the following tasks:

- [Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core, page 27](#)
- [Verifying that the Local and Remote CE Routers are in the Routing Table, page 28](#)

## Verifying IP Connectivity from CE Router to CE Router Across the MPLS Core

Perform this task to verify IP connectivity from CE router to CE router across the MPLS VPN.

### SUMMARY STEPS

1. **enable**

2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]
5. **disable**

## DETAILED STEPS

### Step 1 **enable**

Use this command to enable privileged EXEC mode.

### Step 2 **ping** [*protocol*] {*host-name* | *system-address*}

Use this command to diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. Use the **ping** command to verify the connectivity from one CE router to another.

### Step 3 **trace** [*protocol*] [*destination*]

Use this command to discover the routes that packets take when traveling to their destination. Use the **trace** command to verify the path that a packet goes through before reaching the final destination. The **trace** command can help isolate a trouble spot if two routers cannot communicate.

### Step 4 **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | [*protocol* [*process-id*]] | [**list** *access-list-number* | *access-list-name*]

Use this command to display the current state of the routing table. Use the *ip-address* argument to verify that CE1 has a route to CE2. Verify the routes learned by CE1. Make sure that the route for CE2 is listed.

## Verifying that the Local and Remote CE Routers are in the Routing Table

Perform this task to check that the local and remote CE routers are in the routing table of the PE routers.

## SUMMARY STEPS

1. **enable**
2. **show ip route vrf** *vrf-name* [*prefix*]
3. **show ip cef vrf** *vrf-name* [*ip-prefix*]
4. **exit**

### Step 1 **enable**

Use this command to enable privileged EXEC mode.

### Step 2 **show ip route vrf** *vrf-name* [*prefix*]

Use this command to display the IP routing table associated with a VRF. Check that the loopback addresses of the local and remote CE routers are in the routing table of the PE routers.

### Step 3 **show ip cef vrf** *vrf-name* [*ip-prefix*]

Use this command to display the CEF forwarding table associated with a VRF. Check that the prefix of the remote CE router is in the CEF table.

**Step 4**    **exit**

---

## Configuration Examples for MPLS VPNs

- [Configuring an MPLS VPN Using BGP: Example, page 30](#)
- [Configuring an MPLS VPN Using RIP: Example, page 31](#)
- [Configuring an MPLS VPN Using Static Routes: Example, page 32](#)
- [Configuring an MPLS VPN Using OSPF: Example, page 33](#)
- [Configuring an MPLS VPN Using EIGRP: Example, page 34](#)

## Configuring an MPLS VPN Using BGP: Example

This example shows an MPLS VPN that is configured using BGP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | CE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100   network 10.0.0.0 0.0.0.0 area 100   network 30.0.0.0 0.255.255.255 area 100 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   neighbor 34.0.0.1 remote-as 200   neighbor 34.0.0.1 activate   neighbor 34.0.0.1 as-override   neighbor 34.0.0.1 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router bgp 200   bgp log-neighbor-changes   neighbor 34.0.0.2 remote-as 100 ! address-family ipv4   redistribute connected   neighbor 34.0.0.2 activate   neighbor 34.0.0.2 advertisement-interval 5   no auto-summary   no synchronization   exit-address-family </pre> |

## Configuring an MPLS VPN Using RIP: Example

This example shows an MPLS VPN that is configured using RIP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | CE Configuration                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router rip   version 2   timers basic 30 60 60 120 ! address-family ipv4 vrf vpn1   version 2   redistribute bgp 100 metric transparent   network 34.0.0.0   distribute-list 20 in   no auto-summary   exit-address-family ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute rip   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router rip   version 2   timers basic 30 60 60 120   redistribute connected   network 10.0.0.0   network 34.0.0.0   no auto-summary </pre> |



## Configuring an MPLS VPN Using Static Routes: Example

This example shows an MPLS VPN that is configured using static routes.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | CE Configuration                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip ! router ospf 100 network 10.0.0. 0.0.0.0 area 100 network 30.0.0.0 0.255.255.255 area 100 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute static   no auto-summary   no synchronization   exit-address-family ! ip route vrf vpn1 10.0.0.9 255.255.255.255 34.0.0.1 ip route vrf vpn1 34.0.0.0 255.0.0.0 34.0.0.1 </pre> | <pre> ip cef ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! ip route 10.0.0.9 255.255.255.255 34.0.0.2 3 ip route 31.0.0.0 255.0.0.0 34.0.0.2 3 </pre> |

## Configuring an MPLS VPN Using OSPF: Example

This example shows an MPLS VPN that is configured using OSPF.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | CE Configuration                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 ! interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable ! router ospf 1000 vrf vpn1   log-adjacency-changes   redistribute bgp 100 metric-type 1 subnets   network 10.0.0.13 0.0.0.0 area 10000   network 34.0.0.0 0.255.255.255 area 10000 ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute ospf 1000 match internal   external 1 external 2   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router ospf 1000   log-adjacency-changes   auto-cost reference-bandwidth 1000   redistribute connected subnets   network 34.0.0.0 0.255.255.255 area 1000   network 10.0.0.0 0.0.0.0 area 1000 </pre> |

## Configuring an MPLS VPN Using EIGRP: Example

This example shows an MPLS VPN that is configured using EIGRP.

| PE Configuration                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | CE Configuration                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ip vrf vpn1   rd 100:1   route-target export 100:1   route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.1 255.255.255.255 interface Ethernet0/0   ip vrf forwarding vpn1   ip address 34.0.0.2 255.0.0.0   no cdp enable interface Ethernet 1/1   ip address 30.0.0.1 255.0.0.0   mpls label protocol ldp   mpls ip router eigrp 1000   auto-summary ! address-family ipv4 vrf vpn1   redistribute bgp 100 metric 10000 100 255   1 1500   network 34.0.0.0   distribute-list 20 in   no auto-summary   autonomous-system 1000   exit-address-family ! router bgp 100   no synchronization   bgp log-neighbor changes   neighbor 10.0.0.3 remote-as 100   neighbor 10.0.0.3 update-source Loopback0   no auto-summary ! address-family vpnv4   neighbor 10.0.0.3 activate   neighbor 10.0.0.3 send-community extended   bgp scan-time import 5   exit-address-family ! address-family ipv4 vrf vpn1   redistribute connected   redistribute eigrp   no auto-summary   no synchronization   exit-address-family </pre> | <pre> ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0   ip address 10.0.0.9 255.255.255.255 ! interface Ethernet0/0   ip address 34.0.0.1 255.0.0.0   no cdp enable ! router eigrp 1000   network 34.0.0.0   auto-summary </pre> |

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic                       | Document Title                                                                                                                                                                                                            |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN Carrier Supporting Carrier | <ul style="list-style-type: none"> <li><a href="#">MPLS VPN Carrier Supporting Carrier Using LDP and an IGP</a></li> <li><a href="#">MPLS VPN Carrier Supporting Carrier with BGP</a></li> </ul>                          |
| MPLS VPN InterAutonomous Systems    | <ul style="list-style-type: none"> <li><a href="#">MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</a></li> <li><a href="#">MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</a></li> </ul> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Feature Information for MPLS Layer 3 VPNs

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Layer 3 VPNs

| Feature Name                                                       | Releases                                                                                | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------------------|-----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Virtual Private Networks                                      | 12.0(5)T<br>12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.2(14)S<br>12.0(26)S | This feature allows a set of sites that to be interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">MPLS VPN Definition, page 4</a></li> <li><a href="#">How an MPLS VPN Works, page 5</a></li> <li><a href="#">Major Components of MPLS VPNs, page 7</a></li> <li><a href="#">Benefits of an MPLS VPN, page 7</a></li> <li><a href="#">How to Configure MPLS Layer 3 VPNs, page 9</a></li> </ul> |
| MPLS VPN Support for EIGRP Between Provider Edge and Customer Edge | 12.0(22)S<br>12.2(15)T<br>12.2(18)S<br>12.0(27)S                                        | This feature allows you to connect customers running EIGRP to an MPLS VPN.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li><a href="#">Configuring EIGRP as the Routing Protocol Between the PE and CE Routers, page 23</a></li> <li><a href="#">Configuring EIGRP Redistribution in the MPLS VPN, page 25</a></li> </ul>                                                                                                                                                                                                                                                         |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers,

Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2005-2008 Cisco Systems, Inc. All rights reserved



# MPLS VPN Half-Duplex VRF

---

**First Published: May 2, 2005**

**Last Updated: May 9, 2008**

The MPLS VPN Half-Duplex VRF feature provides scalable hub-and-spoke connectivity for subscribers of an Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) service. This feature addresses the limitations previously imposed on hub-and-spoke topologies by removing the requirement of one Virtual Routing and Forwarding (VRF) per spoke. This feature also ensures that subscriber traffic always traverses the central link between the wholesale service provider and the Internet service provider (ISP), whether the subscriber traffic is being routed to a remote network by way of the upstream ISP or to another locally or remotely connected subscriber.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS VPN Half-Duplex VRF”](#) section on page 18.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for Configuring MPLS VPN Half-Duplex VRF, page 2](#)
- [Restrictions for MPLS VPN Half-Duplex VRF, page 2](#)
- [Information About Configuring MPLS VPN Half-Duplex VRF, page 2](#)
- [How to Configure MPLS VPN Half-Duplex VRF, page 4](#)
- [Configuration Examples for MPLS VPN Half-Duplex VRF, page 10](#)
- [Additional References, page 16](#)
- [Feature Information for MPLS VPN Half-Duplex VRF, page 18](#)



---

**Americas Headquarters:**

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

© 2005–2008 Cisco Systems, Inc. All rights reserved.



# Prerequisites for Configuring MPLS VPN Half-Duplex VRF

You must have a working MPLS core network.

## Restrictions for MPLS VPN Half-Duplex VRF

The following features are not supported on interfaces configured with the MPLS VPN Half-Duplex VRF feature:

- Multicast
- MPLS VPN Carrier Supporting Carrier
- MPLS VPN Interautonomous Systems

## Information About Configuring MPLS VPN Half-Duplex VRF

To configure this feature, you need to understand the following concepts:

- [MPLS VPN Half-Duplex VRF Overview, page 2](#)
- [Upstream and Downstream VRFs, page 3](#)
- [Reverse Path Forwarding Check, page 4](#)

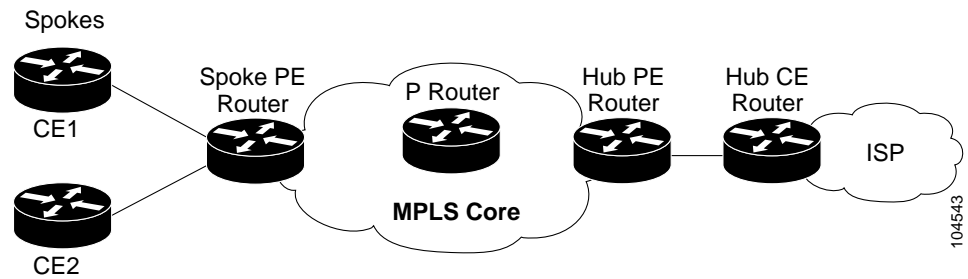
For information about this feature on the Cisco 10000 series routers, see the “Half-Duplex VRF” section of the “Configuring Multiprotocol Label Switching” chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide*.

## MPLS VPN Half-Duplex VRF Overview

The MPLS VPN Half-Duplex VRF feature provides the following benefits:

- The MPLS VPN Half-Duplex VRF feature prevents local connectivity between subscribers at the spoke provider edge (PE) router and ensures that a hub site provides subscriber connectivity. Any sites that connect to the same PE router must forward intersite traffic using the hub site. This ensures that the routing done at the spoke site moves from the access-side interface to the network-side interface or from the network-side interface to the access-side interface, but never from the access-side interface to the access-side interface.
- The MPLS VPN Half-Duplex VRF feature prevents situations where the PE router locally switches the spokes without passing the traffic through the upstream ISP. This prevents subscribers from directly connecting to each other, which causes the wholesale service provider to lose revenue.
- The MPLS VPN Half-Duplex VRF feature improves scalability by removing the requirement of one VRF per spoke. When the feature is not configured, when spokes are connected to the same PE router each spoke is configured in a separate VRF to ensure that the traffic between the spokes traverses the central link between the wholesale service provider and the ISP. However, this configuration is not scalable. When many spokes connected to the same PE router, configuration of VRFs for each spoke becomes quite complex and greatly increases memory usage. This is especially true in large-scale wholesale service provider environments that support high-density remote access to Layer 3 VPNs.

[Figure 1](#) shows a sample hub-and-spoke topology.

**Figure 1**      **Hub-and-Spoke Topology**

## Upstream and Downstream VRFs

The MPLS VPN Half-Duplex VRF feature uses two unidirectional VRFs to forward IP traffic between the spokes and the hub PE router:

- The upstream VRF forwards IP traffic from the spokes toward the hub PE router. This VRF typically contains only a default route but might also contain summary routes and several default routes. The default route points to the interface on the hub PE router that connects to the upstream ISP. The router dynamically learns about the default route from the routing updates that the hub PE router or home gateway sends.



### Note

Although the upstream VRF is typically populated from the hub, it is possible also to have a separate local upstream interface on the spoke PE for a different local service that would not be required to go through the hub: for example, a local Domain Name System (DNS) or game server service.

- The downstream VRF forwards traffic from the hub PE router back to the spokes. This VRF can contain:
  - PPP peer routes for the spokes and per-user static routes received from the authentication, authorization, and accounting (AAA) server or from the Dynamic Host Control Protocol (DHCP) server
  - Routes imported from the hub PE router
  - Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), Routing Information Protocol (RIP), or Enhanced Interior Gateway Routing Protocol (EIGRP) dynamic routes for the spokes

The spoke PE router redistributes routes from the downstream VRF into Multiprotocol Border Gateway Protocol (MP-BGP). That router typically advertises a summary route across the MPLS core for the connected spokes. The VRF configured on the hub PE router imports the advertised summary route.

## Reverse Path Forwarding Check

The Reverse Path Forwarding (RPF) check ensures that an IP packet that enters a router uses the correct inbound interface. The MPLS VPN Half-Duplex VRF feature supports unicast RPF check on the spoke-side interfaces. Because different VRFs are used for downstream and upstream forwarding, the RPF mechanism ensures that source address checks occur in the downstream VRF.

Unicast RPF is not on by default. You need to enable it, as described in [Configuring Unicast Reverse Path Forwarding](#).

## How to Configure MPLS VPN Half-Duplex VRF

This section contains the following procedures:

- [Configuring the Upstream and Downstream VRFs on the Spoke PE Router, page 4](#) (required)
- [Associating a VRF with an Interface, page 6](#) (required)
- [Configuring the Downstream VRF for an AAA Server, page 7](#) (optional)
- [Verifying MPLS VPN Half-Duplex VRF Configuration, page 7](#) (optional)

To configure this feature on the Cisco 10000 series routers, see the “Half-Duplex VRF” section of the “Configuring Multiprotocol Label Switching” chapter in the [Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide](#).

## Configuring the Upstream and Downstream VRFs on the Spoke PE Router

To configure the upstream and downstream VRFs on the PE router or on the spoke PE router, use the following procedure.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit-address-family**
8. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>vrf definition vrf-name</b><br><br><b>Example:</b><br>Router(config)# vrf definition vrf1                                                               | Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name of the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 4 | <b>rd route-distinguisher</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1                                                                       | Creates routing and forwarding tables for a VRF. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument specifies to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats: <ul style="list-style-type: none"> <li>16-bit autonomous system number (ASN): your 32-bit number<br/>For example, 101:3.</li> <li>32-bit IP address: your 16-bit number<br/>For example, 192.168.122.15:1.</li> </ul> </li> </ul>                                                                                                                                                                       |
| Step 5 | <b>address-family {ipv4   ipv6}</b><br><br><b>Example:</b><br>Router(config-vrf) address-family ipv4                                                       | Enters VRF address family configuration mode to specify an address family for a VRF. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies an IPv4 address family for a VRF.</li> <li>The <b>ipv6</b> keyword specifies an IPv6 address family for a VRF.</li> </ul> <p><b>Note</b> The MPLS VPN Half Duplex VRF feature supports only IPv4 address family.</p>                                                                                                                                                                                                                                                                                                      |
| Step 6 | <b>route-target {import   export   both}</b><br><b>route-target-ext-community</b><br><br><b>Example:</b><br>Router(config-vrf-af)# route-target both 100:2 | Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword specifies to import routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword specifies to export routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword specifies to import both import and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |

|        | Command or Action                                                                               | Purpose                                           |
|--------|-------------------------------------------------------------------------------------------------|---------------------------------------------------|
| Step 7 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-vrf-af)# exit-address-family | Exits from VRF address family configuration mode. |
| Step 8 | <b>end</b><br><br><b>Example:</b><br>Router(config-vrf-af)# end                                 | Exits to privileged EXEC mode.                    |

## Associating a VRF with an Interface

Perform the following task to associate a VRF with an interface, which activates the VRF.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [secondary]
6. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                           | Enters global configuration mode.                                                                                                                                                                                                                                                                     |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/1                                     | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <b>type</b> argument identifies the type of interface to be configured.</li> <li>• The <b>number</b> argument identifies the port, connector, or interface card number.</li> </ul> |
| Step 4 | <b>vrf forwarding</b> <i>vrf-name</i> [ <b>downstream</b> <i>vrf2</i> ]<br><br><b>Example:</b><br>Router(config-if)# vrf forwarding vrf1 | Associates a VRF with an interface or subinterface. <ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is the name of the VRF.</li> <li>• The <b>downstream</b> <i>vrf2</i> is the name of the downstream VRF into which peer and per-user routes are installed.</li> </ul>        |

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.24.24.24 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask of the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-if) end                                                                                        | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                               |

## Configuring the Downstream VRF for an AAA Server

To configure the downstream VRF for an AAA (RADIUS) server in broadband or remote access situations, enter the following Cisco attribute value:

**lcp:interface-config=ip vrf forwarding U downstream D**

In standard VPN situations, enter instead the following Cisco attribute value:

**ip:vrf-id=U downstream D**

## Verifying MPLS VPN Half-Duplex VRF Configuration

To verify the Downstream VRF for an AAA Server configuration, perform the following steps.

### SUMMARY STEPS

1. **show vrf** [**brief** | **detail** | **id** | **interfaces** | **lock** | **select** ] [*vrf-name*]
2. **show ip route vrf** *vrf-name*
3. **show running-config** [**interface** *type number*]

### DETAILED STEPS

**Step 1** **show vrf** [**brief** | **detail** | **id** | **interfaces** | **lock** | **select** ] [*vrf-name*]

Use this command to display information about all of the VRFs configured on the router, including the downstream VRF for each associated interface or VAI:

Router# **show vrf**

```

Name      Default RD      Interfaces
Down      100:1           POS3/0/3 [D]
                        POS3/0/1 [D]
                        100:3          Loopback2
                        Virtual-Access3 [D]
```

```

Up      100:2      Virtual-Access4 [D]
          POS3/0/3
          POS3/0/1
          100:4      Virtual-Access3

```

### **show vrf detail vrf-name**

Use this command to display detailed information about the VRF you specify, including all interfaces, subinterfaces, and VAIs associated with the VRF.

If you do not specify a value for the *vrf-name* argument, detailed information about all of the VRFs configured on the router appears.

The following example shows how to display detailed information for the VRF called vrf1, in a broadband or remote access case:

```

Router# show vrf detail vrf1

VRF D; default RD 2:0; default VPNID <not set>
  Interfaces:
    Loopback2          Virtual-Access3 [D]  Virtual-Access4 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:0
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
VRF U; default RD 2:1; default VPNID <not set>
  Interfaces:
    Virtual-Access3      Virtual-Access4
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map

```

The following example shows the VRF detail in a standard VPN situation:

```

Router# show vrf detail

VRF Down; default RD 100:1; default VPNID <not set> VRF Table ID = 1
  Description: import only from hub-pe
  Interfaces:
    Pos3/0/3 [D]          Pos3/0/1:0.1 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:0
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF Up; default RD 100:2; default VPNID <not set> VRF Table ID = 2
  Interfaces:
    Pos3/0/1          Pos3/0/3
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured

```

**Step 2** **show ip route vrf vrf-name**

Use this command to display the IP routing table for the VRF you specify, and information about the per-user routes installed in the downstream VRF.

The following example shows how to display the routing table for the downstream VRF named D, in a broadband or remote access situation:

```
Router# show ip route vrf D
```

```
Routing Table: D
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
```

Gateway of last resort is not set

```
10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U    10.0.0.2/32 [1/0] via 10.0.0.1
S    10.0.0.0/8 is directly connected, Null0
U    10.0.0.5/32 [1/0] via 10.0.0.2
C    10.8.1.2/32 is directly connected, Virtual-Access4
C    10.8.1.1/32 is directly connected, Virtual-Access3
```

The following example shows how to display the routing table for the downstream VRF named Down, in a standard VPN situation:

```
Router# show ip route vrf Down
```

```
Routing Table: Down
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.13.13.13 to network 0.0.0.0

```
C    10.2.0.0/8 is directly connected, Pos3/0/3
     10.3.0.0/32 is subnetted, 1 subnets
B    10.4.16.16 [200/0] via 10.13.13.13, 1w3d
B    10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
C    10.0.0.0/8 is directly connected, Pos3/0/1
     10.7.0.0/16 is subnetted, 1 subnets
B    10.7.0.0 [20/0] via 10.0.0.2, 1w3d
     10.0.6.0/32 is subnetted, 1 subnets
B    10.0.6.14 [20/0] via 10.0.0.2, 1w3d
     10.8.0.0/32 is subnetted, 1 subnets
B    10.8.15.15 [20/0] via 10.0.0.2, 1w3d
B*   0.0.0.0/0 [200/0] via 10.0.0.13, 1w3d
```

The following example shows how to display the routing table for the upstream VRF named U in a broadband or remote access situation:

```
Router# show ip route vrf U
```

```
Routing Table: U
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
```



```

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

```

Gateway of last resort is 192.168.0.20 to network 0.0.0.0

```

10.0.0.0/32 is subnetted, 1 subnets
C    10.0.0.8 is directly connected, Loopback2
B*   0.0.0.0/0 [200/0] via 192.168.0.20, 1w5d

```

The following example shows how to display the routing table for the upstream VRF named Up in a standard VPN situation:

Router# **show ip route vrf Up**

```

Routing Table: Up
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route

```

Gateway of last resort is 10.13.13.13 to network 0.0.0.0

```

10.2.0.0/32 is subnetted, 1 subnets
C    10.2.0.1 is directly connected, Pos3/0/3
10.3.0.0/32 is subnetted, 1 subnets
B    10.3.16.16 [200/0] via 10.13.13.13, 1w3d
B    10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
10.0.0.0/32 is subnetted, 1 subnets
C    10.0.0.1 is directly connected, Pos3/0/1
B*   0.0.0.0/0 [200/0] via 10.13.13.13, 1w3d

```

### Step 3 **show running-config [interface type number]**

Use this command to display information about the interface you specify, including information about the associated upstream and downstream VRFs.

The following example shows how to display information about the subinterface named POS3/0/1:

Router# **show running-config interface POS3/0/1**

Building configuration...

```

Current configuration : 4261 bytes
!
interface POS3/0/1
    ip vrf forwarding Up downstream Down
    ip address 10.0.0.1 255.0.0.0
end

```

## Configuration Examples for MPLS VPN Half-Duplex VRF

This section provides the following configuration examples:

- [Configuring the Upstream and Downstream VRFs on the Spoke PE Router: Example, page 11](#)
- [Associating a VRF with an Interface: Example, page 11](#)
- [Configuring MPLS VPN Half-Duplex VRF: Example Using Static CE-PE Routing, page 11](#)
- [Configuring MPLS VPN Half-Duplex VRF: Example Using RADIUS Server and Static CE-PE Routing, page 13](#)
- [Configuring MPLS VPN Half-Duplex VRF: Example Using Dynamic CE-PE Routing, page 14](#)

## Configuring the Upstream and Downstream VRFs on the Spoke PE Router: Example

The following example configures an upstream VRF named Up:

```
Router> enable
Router# configure terminal
Router(config)# vrf definition Up
Router(config-vrf)# rd 1:0
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# route-target import 1:0
Router(config-vrf-af)# exit-address-family
```

The following example configures a downstream VRF named Down:

```
Router> enable
Router# configure terminal
Router(config)# vrf definition Down
Router(config-vrf)# rd 1:8
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# route-target import 1:8
Router(config-vrf-af)# exit-address-family
```

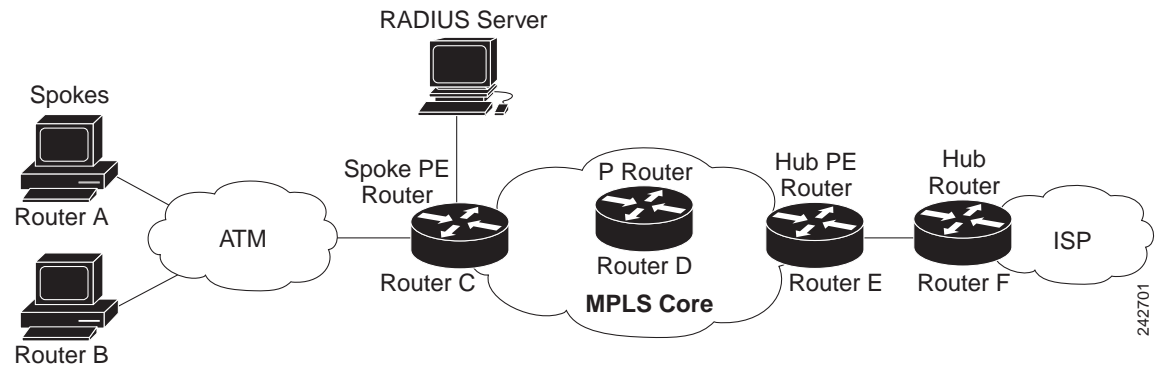
## Associating a VRF with an Interface: Example

The following example associates the VRF named Up with the POS3/0/1 subinterface and specifies the downstream VRF named Down:

```
Router> enable
Router# configure terminal
Router(config)# interface POS 3/0/1
Router(config-if)# vrf forwarding Up downstream Down
Router(config-if)# ip address 10.0.0.1 255.0.0.0
```

## Configuring MPLS VPN Half-Duplex VRF: Example Using Static CE-PE Routing

This example uses the hub-and-spoke topology shown in [Figure 2](#) with local authentication (that is, the RADIUS server is not used).

**Figure 2 Sample Topology**

```

vrf definition D
 rd 1:8
 address-family ipv4
 route-target export 1:100
 exit-address-family
!
vrf definition U
 rd 1:0
 address-family ipv4
 route-target import 1:0
 exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
 protocol pppoe
 virtual-template 1
!
interface Loopback2
 vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
 description Mze ATM3/1/2
 no ip address
 no atm ilmi-keepalive
 pvc 0/16 ilmi
!
 pvc 3/100
 protocol pppoe
!
 pvc 3/101
 protocol pppoe
!

```

## Configuring MPLS VPN Half-Duplex VRF: Example Using RADIUS Server and Static CE-PE Routing

The following example shows how to connect two Point-to-Point Protocol over Ethernet (PPPoE) clients to a single VRF pair on the spoke PE router named Router C. Although both PPPoE clients are configured in the same VRF, all communication occurs using the hub PE router. Half-duplex VRFs are configured on the spoke PE. The client configuration is downloaded to the spoke PE from the RADIUS server.

This example uses the hub-and-spoke topology shown in [Figure 2](#).



### Note

The wholesale provider can forward the user authentication request to the corresponding ISP. If the ISP authenticates the user, the wholesale provider appends the VRF information to the request that goes back to the PE router.

```

aaa new-model
!
aaa group server radius R
  server 10.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
vrf definition D
  description Downstream VRF - to spokes
  rd 1:8
  address-family ipv4
  route-target export 1:100
  exit-address-family
!
vrf definition U
  description Upstream VRF - to hub
  rd 1:0
  address-family ipv4
  route-target import 1:0
  exit-address-family
!
ip cef
vpdn enable
!
vpdn-group U
  accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback2
  vrf forwarding U
  ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
  pvc 3/100
  protocol pppoe
!
pvc 3/101
  protocol pppoe
!
interface virtual-template 1
  no ip address
  ppp authentication chap

```

```

!
router bgp 1
  no synchronization
  neighbor 172.16.0.34 remote-as 1
  neighbor 172.16.0.34 update-source Loopback0
  no auto-summary
!
address-family vpnv4
  neighbor 172.16.0.34 activate
  neighbor 172.16.0.34 send-community extended
  auto-summary
  exit-address-family
!
address-family ipv4 vrf U
  no auto-summary
  no synchronization
  exit-address-family
!
address-family ipv4 vrf D
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool U-pool 10.8.1.1 2.8.1.100
ip route vrf D 10.0.0.0 255.0.0.0 Null0
!
radius-server host 10.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco

```

## Configuring MPLS VPN Half-Duplex VRF: Example Using Dynamic CE-PE Routing

The following example shows how to use OSPF to dynamically advertise the routes on the spoke sites.

This example uses the hub-and-spoke topology shown in [Figure 2](#).

### Creating the VRFs

```

vrf definition Down
  rd 100:1
  address-family ipv4
  route-target export 100:0
  exit-address-family
!
vrf definition Up
  rd 100:2
  address-family ipv4
  route-target import 100:1
  exit-address-family

```

### Enabling MPLS

```

mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp

```

### Configuring BGP Toward Core

```

router bgp 100
  no bgp default ipv4-unicast

```

```

bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 10.13.13.13 remote-as 100
neighbor 10.13.13.13 update-source Loopback0
!
address-family vpnv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
bgp scan-time import 5
exit-address-family

```

### Configuring BGP Toward Edge

```

address-family ipv4 vrf Up
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf Down
redistribute ospf 1000 vrf Down
no auto-summary
no synchronization
exit-address-family

```

### Spoke PE's Core-Facing Interfaces and Processes

```

interface Loopback0
    ip address 10.11.11.11 255.255.255.255
!
interface POS3/0/2
    ip address 10.0.1.1 255.0.0.0
    mpls label protocol ldp
    mpls ip
!
router ospf 100
    log-adjacency-changes
    auto-cost reference-bandwidth 1000
    nsf enforce global
    redistribute connected subnets
    network 10.11.11.11 0.0.0.0 area 100
    network 10.0.1.0 0.255.255.255 area 100

```

### Spoke PE's Edge-Facing Interfaces and Processes

```

interface Loopback100
    vrf forwarding Down
    ip address 10.22.22.22 255.255.255.255
!
interface POS3/0/1
    vrf forwarding Up downstream Down
    ip address 10.0.0.1 255.0.0.0
!
interface POS3/0/3
    vrf forwarding Up downstream Down
    ip address 10.2.0.1 255.0.0.0
!
router ospf 1000 vrf Down
    router-id 10.22.22.22
    log-adjacency-changes
    auto-cost reference-bandwidth 1000
    nsf enforce global
    redistribute connected subnets

```

```

redistribute bgp 100 metric-type 1 subnets
network 10.22.22.22 0.0.0.0 area 300
network 10.0.0.0 0.255.255.255 area 300
network 10.2.0.0 0.255.255.255 area 300
default-information originate

```

## Additional References

The following sections provide references related to the MPLS VPN Half-Duplex VRFs feature.

## Related Documents

| Related Topic                   | Document Title                                                            |
|---------------------------------|---------------------------------------------------------------------------|
| MPLS VPNs                       | <a href="#">Configuring MPLS Layer 3 VPNs</a>                             |
| MPLS commands                   | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |
| Configuring IPv4 and IPv6 VRFs  | <a href="#">MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs</a>                   |
| Unicast Reverse Path Forwarding | <a href="#">Configuring Unicast Reverse Path Forwarding</a>               |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                |
|----------|--------------------------------------|
| RFC 2547 | <a href="#"><i>BGP/MPLS VPNs</i></a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |



# Feature Information for MPLS VPN Half-Duplex VRF

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN Half-Duplex VRF

| Feature Name                                                   | Releases                                | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN - Half Duplex VRF (HDVRF) Support with Static Routing | 12.3(6)<br>12.3(11)T<br>12.2(28)SB      | This feature ensures that VPN clients that connect to the same PE router at the edge of the MPLS VPN use the hub site to communicate.<br><br>In 12.3(6), this feature was introduced.<br><br>In 12.4(20)T, this feature was integrated.<br><br>In 12.2(28)SB, this feature was integrated                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| MPLS VPN Half-Duplex VRF                                       | 12.2(28)SB2<br>12.4(20)T<br>12.2(33)SRC | In 12.2(28)SB2, support for dynamic routing protocols was added.<br><br>For the Cisco 10000 series routers, see the “Half-Duplex VRF” section of the “Configuring Multiprotocol Label Switching” chapter in the <i>Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide</i> at the following URL:<br><a href="http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/dffsrv.htm#wp1065648">http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/dffsrv.htm#wp1065648</a><br><br>In 12.4(20)T, this feature, with support for dynamic routing protocols, was integrated.<br><br>In Cisco IOS Release 12.2(33)SRC this feature, with support for dynamic routing protocols, was integrated into the SR train.<br><br>The following commands were introduced or modified:<br><b>show ip interface, show vrf</b> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA,

CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.





# MPLS VPN—Show Running VRF

---

**First Published: March 16, 2006**

**Last Updated: July 11, 2008**

The MPLS VPN—Show Running VRF feature provides a Cisco IOS command-line interface (CLI) option to display a subset of the running configuration on a router that is linked to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. You can display the configuration of a specific VRF or of all VRFs configured on a router.

On heavily loaded routers, the display of the configuration file might require several pages or screens. As the configuration increases in size and complexity, the possibility of misconfiguration also increases. You might find it difficult to trace a problem on a router where you have several VRFs configured. A command that displays all the elements of the configuration linked to a VRF allows for easier troubleshooting on a per-VRF basis and facilitates comparisons among configurations of different VRFs on the same router.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS VPN—Show Running VRF](#)” section on [page 6](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS VPN—Show Running VRF, page 2](#)
- [Restrictions for MPLS VPN—Show Running VRF, page 2](#)
- [Information About MPLS VPN—Show Running VRF, page 2](#)
- [How to Configure MPLS VPN—Show Running VRF, page 4](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for MPLS VPN—Show Running VRF, page 4](#)
- [Additional References, page 4](#)
- [Command Reference, page 5](#)
- [Feature Information for MPLS VPN—Show Running VRF, page 6](#)
- [Glossary, page 8](#)

## Prerequisites for MPLS VPN—Show Running VRF

- A Cisco IOS image that supports VRFs installed on the router
- At least one VRF configured on the router
- Cisco Express Forwarding for MPLS VPN routing and forwarding

## Restrictions for MPLS VPN—Show Running VRF

Any element of the running configuration of the router that is not linked directly to a VRF is not displayed. For example, a route map associated with a Border Gateway Protocol (BGP) neighbor in a VRF address-family configuration is not displayed. The VRF address-family configuration under BGP is displayed, but the route-map configuration is not. An exception to this general rule is the display of a controller configuration (for more information, see the [“Display of Configuration Not Directly Linked to a VRF”](#) section on page 4).

## Information About MPLS VPN—Show Running VRF

Before using the MPLS VPN—Show Running VRF feature, you should understand the following information:

- [Configuration Elements Displayed for the MPLS VPN—Show Running VRF Feature, page 2](#)
- [Display of VRF Routing Protocol Configuration, page 3](#)
- [Display of Configuration Not Directly Linked to a VRF, page 4](#)

## Configuration Elements Displayed for the MPLS VPN—Show Running VRF Feature

You can display the running configuration associated with a specific VRF or all VRFs on the router by entering the **show running-config vrf** command. To display the running configuration of a specific VRF, enter the name of the VRF as an argument to the **show running-config vrf** command. For example, for a VRF named vpn3, you enter:

```
Router# show running-config vrf vpn3
```

The **show running-config vrf** command displays the following elements of the running configuration on a router:

- The VRF configuration

This includes any configuration that is applied in the VRF submode.

- The configuration of each interface in the VRF

Entering a **show run vrf vpn-name** command is the same as executing a **show running-config interface type number** for each interface that you display by use of the **show ip vrf vpn-name** command. The interfaces display in the same sorted order that you would expect from the **show ip interface** command.

For a channelized interface, the configuration of the controller is displayed (as shown by the **show run controller controller-name** command).

For a subinterface, the configuration of the main interface is displayed.

- The configuration of routing-protocol address families or processes that are linked with the VRF, including static routing configuration (see the [“Display of VRF Routing Protocol Configuration” section on page 3](#))

## Display of VRF Routing Protocol Configuration

Open Shortest Path First (OSPF), Routing Information Protocol (RIP), Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), and static routing are routing protocols that support VRF configuration.

OSPF has one process per VRF. The **show running-config vrf** command display includes the complete configuration of any OSPF process associated with the VRF. For example, the following shows the sample display for OSPF process 101, which is associated with the VRF named vpn3:

```
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
```

RIP, BGP, and EIGRP support VRF address-family configuration. If a VRF address family for the VRF exists for any of these routing protocols, a configuration in the following format is displayed:

```
router protocol {AS | PID}
!
address-family ipv4 vrf vrf-name
.
.
.
```

Where the *protocol* argument is one of the following: **rip**, **bgp** or **eigrp**; the *AS* argument is an autonomous system number; the *PID* argument is a process identifier; and the *vrf-name* argument is the name of the associated VRF.

The following shows a sample display for a BGP with autonomous system number 100 associated with a VRF named vpn3:

```
!
router bgp 100
!
address-family ipv4 vrf vpn3
 redistribute connected
 redistribute ospf 101 match external 1 external 2
 no auto-summary
```

```
no synchronization
exit-address-family
!
```

The **show running-config vrf** command also includes the configuration of any static routes configured in the VRF. For example:

```
ip route vrf vpn1 10.1.1.0 255.255.255.0 10.30.1.1 global
ip route vrf vpn1 10.1.2.0 255.255.255.0 10.125.1.2
```

## Display of Configuration Not Directly Linked to a VRF

Any element of a configuration that is not linked directly to a VRF is not displayed. In some instances, the display of the configuration of an element that is not directly linked to a VRF is required.

For example, the **show running-config vrf** command displays the configuration of an E1 controller whose serial subinterfaces are in a VRF. The command displays the controller configuration and the subinterface configuration.

## How to Configure MPLS VPN—Show Running VRF

There are no tasks for the MPLS VPN—Show Running VRF feature.

## Configuration Examples for MPLS VPN—Show Running VRF

There are no configuration examples for the MPLS VPN—Show Running VRF feature.

## Additional References

The following sections provide references related to the MPLS VPN—Show Running VRF feature.

### Related Documents

| Related Topic             | Document Title                                                            |
|---------------------------|---------------------------------------------------------------------------|
| MPLS command descriptions | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a> |

### Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **show policy-map interface brief**
- **show running-config vrf**



# Feature Information for MPLS VPN—Show Running VRF

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—Show Running VRF

| Feature Name              | Releases                                                            | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Show Running VRF | 12.2(28)SB<br>12.0(32)SY<br>12.2(33)SRB<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS VPN—Show Running VRF feature provides a CLI option to display a subset of the running configuration on a router that is linked to a VRF. You can display the configuration of a specific VRF or of all VRFs configured on a router. A command that displays all the elements of the configuration linked to a VRF allows for easier troubleshooting on a per-VRF basis and facilitates comparisons among configurations of different VRFs on the same router.</p> <p>In 12.2(28)SB, this feature was introduced.</p> <p>In 12.0(32)SY, support was added for a Cisco IOS 12.0SY release.</p> <p>In 12.2(33)SRB, support was added for a Cisco IOS 12.2SR release.</p> <p>In 12.2(33)SXH, support was added for a Cisco IOS 12.2SX release.</p> <p>In 12.4(20)T, support was added for a Cisco IOS 12.4T release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Configuration Elements Displayed for the MPLS VPN—Show Running VRF Feature, page 2</a></li> <li>• <a href="#">Display of VRF Routing Protocol Configuration, page 3</a></li> <li>• <a href="#">Display of Configuration Not Directly Linked to a VRF, page 4</a></li> </ul> |

**Table 1**      *Feature Information for MPLS VPN—Show Running VRF (continued)*

| Feature Name | Releases | Feature Information                                                                                                              |
|--------------|----------|----------------------------------------------------------------------------------------------------------------------------------|
|              |          | The following commands were introduced or modified:<br><b>show policy-map interface brief</b> , <b>show running-config vrf</b> . |

# Glossary

**BGP**—Border Gateway Protocol. An interdomain routing protocol that replaces External Gateway Protocol (EGP). BGP systems exchange reachability information with other BGP systems. BGP is defined by RFC 1163.

**EGP**—External Gateway Protocol. An internet protocol for exchanging routing information between autonomous systems. EGP is documented in RFC 904. Not to be confused with the general term exterior gateway protocol. EGP is an obsolete protocol that was replaced by Border Gateway Protocol (BGP).

**EIGRP**—Enhanced Interior Gateway Routing Protocol. Advanced version of Interior Gateway Routing Protocol (IGRP) developed by Cisco. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.

**IGP**—Interior Gateway Protocol. An internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**IGRP**—Interior Gateway Routing Protocol. An Interior Gateway Protocol (IGP) developed by Cisco to address the issues associated with routing in large, heterogeneous networks.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic through the use of a label. This label instructs the routers and the switches in the network where to forward each packet based on preestablished IP routing information.

**OSPF**—Open Shortest Path First. A link-state, hierarchical, Interior Gateway Protocol (IGP) routing algorithm and routing protocol proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the Intermediate System-to-Intermediate System (IS-IS) protocol.

**RIP**—Routing Information Protocol. Internal Gateway Protocol (IGP) supplied with UNIX Berkeley Software Distribution (BSD) systems. RIP is the most common IGP in the Internet. It uses hop count as a routing metric.

**VPN**—Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF**—A Virtual Private Network (VPN) routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.



# MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

---

**First Published: February 19, 2007**

**Last Updated: November 7, 2008**

This document describes how to configure a Virtual Private Network (VPN) routing and forwarding (VRF) instance for IPv4 and IPv6 VPNs and describes how to upgrade your existing single-protocol IPv4-only VRF to a multiprotocol VRF configuration.

The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature introduces Cisco IOS command-line interface (CLI) commands that allow you to enable an IPv4 and IPv6 VPN in the same VRF instance and to simplify the migration from a single-protocol VRF configuration to a multiprotocol VRF configuration.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs](#)” section on [page 19](#).

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

## Contents

- [Prerequisites for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 2](#)
- [Restrictions for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 2](#)
- [Information About MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 2](#)
- [How to Configure MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 6](#)
- [Configuration Examples for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 14](#)



---

**Americas Headquarters:**

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

- [Additional References, page 17](#)
- [Command Reference, page 18](#)
- [Feature Information for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs, page 19](#)
- [Glossary, page 21](#)

## Prerequisites for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature has the following prerequisites:

- For migration—An IPv4 Multiprotocol Label Switching (MPLS) VPN VRF must exist.
- For a new VRF configuration—Cisco Express Forwarding and an MPLS label distribution method, either Label Distribution Protocol (LDP) or MPLS traffic engineering (TE), must be enabled on all routers in the core, including the provider edge (PE) routers.

## Restrictions for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature has the following restrictions:

- Once you have converted to a multiprotocol VRF, you cannot convert the VRF back to an IPv4-only single-protocol VRF.
- You can associate an interface with only one VRF. You cannot configure a VRF for IPv4 and a different VRF for IPv6 on the same interface.
- You can configure only IPv4 and IPv6 address families in a multiprotocol VRF. Other protocols (IPX, AppleTalk, and the like) are not supported.

## Information About MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

Before you use the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature to migrate from a single-protocol VRF to a multiprotocol VRF, you should understand the following concepts:

- [VRF Concepts Similar for IPv4 and IPv6 MPLS VPNs, page 2](#)
- [Single-Protocol VRF to Multiprotocol VRF Migration, page 3](#)
- [Multiprotocol VRF Configurations Characteristics and Examples, page 4](#)

## VRF Concepts Similar for IPv4 and IPv6 MPLS VPNs

VPNs for IPv6 use the same VRF concepts that IPv4 MPLS VPNs use, such as address families, route distinguishers, route targets, and VRF identifiers. Customers that use both IPv4 and IPv6 VPNs might want to share VRF policies between address families. They might want a way to define applicable VRF policies for all address families, instead of defining VRF policies for an address family individually as they do for or a single-protocol IPv4-only VRF.

Prior to Cisco IOS Release 12.2(33)SRB, a VRF applied only to an IPv4 address family. A one-to-one relationship existed between the VRF name and a routing and forwarding table identifier, between a VRF name and a route distinguisher (RD), and between a VRF name and a VPN ID. This configuration is called a single-protocol VRF.

Cisco IOS Release 12.2(33)SRB introduces support for a multiple address-family (multi-AF) VRF structure. The multi-AF VRF allows you to define multiple address families under the same VRF. A given VRF, identified by its name and a set of policies, can apply to both an IPv4 VPN and an IPv6 VPN at the same time. This VRF can be activated on a given interface, even though the routing and forwarding tables are different for the IPv4 and IPv6 protocols. This configuration is called a multiprotocol VRF.

## Single-Protocol VRF to Multiprotocol VRF Migration

Prior to Cisco IOS Release 12.2(33)SRB, you could create a single-protocol IPv4-only VRF. You created a single-protocol VRF by entering the **ip vrf** command. To activate the single-protocol VRF on an interface, you entered the **ip vrf forwarding** (interface configuration) command.

After the introduction of the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature in Cisco IOS Release 12.2(33)SRB, you create a multiprotocol VRF by entering the **vrf definition** command. To activate the multiprotocol VRF on an interface, you enter the **vrf forwarding** command.

The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature introduces the **vrf upgrade-cli multi-af-mode {common-policies | non-common-policies} [vrf vrf-name]** command that forces VRF configuration migration from a single-protocol VRF model to a multiprotocol VRF model:

- If the route-target policies apply to all address families configured in the multi-AF VRF, select the **common-policies** keyword.
- If the route-target policies apply only to the IPv4 address family that you are migrating, select the **non-common-policies** keyword.

After you enter the **vrf upgrade-cli** command and save the configuration to NVRAM, the single-protocol VRF configuration is saved as a multiprotocol VRF configuration. In the upgrade process, the **ip vrf** command is converted to the **vrf definition** command (global configuration commands) and the **ip vrf forwarding** command is converted to the **vrf forwarding** command (interface configuration command). The **vrf upgrade-cli** command has a one-time immediate effect.

You might have both IPv4-only VRFs and multiprotocol VRFs on your router. Once you create a VRF, you can edit it using only the commands in the mode in which it was created. For example, you created a VRF named vrf2 with the following multiprotocol VRF commands:

```
Router# configure terminal
Enter configuration command, one per line. End with CNTL/Z
Router(config)# vrf definition vrf2
Router(config-vrf)# rd 2:2
Router(config-vrf)# route-target import 2:2
Router(config-vrf)# route-target export 2:2
Router(config-vrf)# end
```

If you try to edit VRF vrf2 with IPv4-only VRF commands, you receive the following message:

```
Router# configure terminal
Enter configuration command, one per line. End with CNTL/Z
Router(config)# ip vrf vrf2
```

% Use 'vrf definition vrf2' command

If you try to edit an IPv4-only VRF with the multiprotocol VRF commands, you would receive this message, where <vrf-name> is the name of the IPv4-only VRF:

% Use 'ip vrf <vrf-name>' command

The **ip vrf name** and **ip vrf forwarding** (interface configuration) *name* commands will be available for a period of time before they are removed. Use the **vrf upgrade** command to migrate your older IPv4-only VRFs to the new multiprotocol VRF configuration. When you need to create a new VRF—whether the VRF is for an IPv4 VPN, or IPv6 VPN, or both—use the multiprotocol VRF **vrf definition** and **vrf forwarding** commands that support a multi-AF configuration.

## Multiprotocol VRF Configurations Characteristics and Examples

In a multiprotocol VRF, you can configure both IPv4 VRFs and IPv6 VRFs under the same address family or configure separate VRFs for each IPv4 or IPv6 address family. The multiprotocol VRF configuration has the following characteristics:

- The VRF name identifies a VRF, which might have both IPv4 and IPv6 address families. On the same interface, you cannot have IPv4 and IPv6 address families using different VRF names.
- The RD, VPN ID, and Simple Network Management Protocol (SNMP) context are shared by both IPv4 and IPv6 address families for a given VRF.
- The policies (route target, for example) specified in multi-AF VRF mode, outside the address-family configuration, are defaults to be applied to each address family. Route targets are the only VRF characteristics that can be defined inside and outside an address family.

The following is also true when you associate a multiprotocol VRF with an interface:

- Binding an interface to a VRF (**vrf forwarding vrf-name** command) removes all IPv4 and IPv6 addresses configured on that interface.
- Once you associate a VRF with a given interface, all active address families belong to that VRF. The exception is when no address of the address-family type is configured, in which case the protocol is disabled.
- Configuring an address on an interface that is bound to a VRF requires that the address family corresponding to the address type is active for that VRF. Otherwise, an error message is issued stating that the address family must be activated first in the VRF.

Backward compatibility with the single-protocol VRF CLI is supported in Cisco IOS Release 12.2(33)SRB. This means that you might have single-protocol and multiprotocol CLI on the same router, but not in the same VRF configuration.

The single-protocol CLI continues to allow you to define an IPv4 address within a VRF and an IPv6 address in the global routing table on the same interface.

The following sections have multiprotocol VRF configuration examples:

- [Multiprotocol VRF Configuration: Single Protocol with Noncommon Policies Example, page 4](#)
- [Multiprotocol VRF Configuration: Multiprotocol with Noncommon Policies Example, page 5](#)
- [Multiprotocol VRF Configuration: Multiprotocol with Common Policies Example, page 5](#)
- [Multiprotocol VRF Configuration: Multiprotocol with Common and Noncommon Policies, page 5](#)

### Multiprotocol VRF Configuration: Single Protocol with Noncommon Policies Example

The following is an example of a multiprotocol VRF configuration for a single protocol (IPv4) with route-target policies in the address-family configuration:

```
vrf definition vrf2
rd 2:2
!
address-family ipv4
```

```
route-target export 2:2
route-target import 2:2
exit-address-family
```

The RD (2:2) applies to all address families defined for VRF vrf2.

## Multiprotocol VRF Configuration: Multiprotocol with Noncommon Policies Example

The following is an example of a multiprotocol VRF configuration for IPv4 and IPv6 VPNs in which the route-target policies are defined in the separate address-family configurations:

```
vrf definition vrf2
 rd 2:2
 !
 address-family ipv4
  route-target export 2:2
  route-target import 2:2
 exit-address-family
 !
 address-family ipv6
  route-target export 3:3
  route-target import 3:3
 exit-address-family
```

## Multiprotocol VRF Configuration: Multiprotocol with Common Policies Example

The following is an example of a multiprotocol VRF configuration for IPv4 and IPv6 VPNs with route-target policies defined in the global part of the VRF:

```
vrf definition vrf2
 rd 2:2
 route-target export 2:2
 route-target import 2:2
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
```

The route-target policies are defined outside the address-family configurations. Therefore, the policies apply to all address families defined in VRF vrf2.

## Multiprotocol VRF Configuration: Multiprotocol with Common and Noncommon Policies

The following is an example of a multiprotocol VRF with route-target policies defined in both global and address-family areas:

- For IPv6, the route-target definitions are defined under the address family. These definitions are used and the route-target definitions in the global area are ignored. Therefore, the IPv6 VPN ignores import 100:2.
- For IPv4, no route-target policies are defined under the address family, therefore, the global definitions are used.

```
vrf definition vrf1
 route-target export 100:1
 route-target import 100:1
 route-target import 100:2
 !
```



```

address-family ipv4
exit-address-family
!
address-family ipv6
route-target export 100:1
route-target import 100:1
route-target import 100:3
exit-address-family

```

## How to Configure MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

This feature provides Cisco IOS CLI commands that allow you to configure a multiprotocol VRF (IPv4 and IPv6 VPNs in the same VRF) and to migrate a single-protocol VRF configuration (IPv4-only VRF) to a multiprotocol VRF configuration.

A multiprotocol VRF allows you to share route targets policies (import and export) between IPv4 and IPv6 or to configure separate route-target policies for IPv4 and IPv6 VPNs.

Perform the tasks in the following sections to configure or migrate to the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature:

- [Configuring a VRF for IPv4 and IPv6 MPLS VPNs, page 6](#) (required)
- [Associating a Multiprotocol VRF with an Interface, page 9](#) (required)
- [Verifying the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs Configuration, page 10](#) (optional)

Perform the following task to migrate from a single-protocol VRF to a multiprotocol VRF configuration:

- [Migrating from a Single-Protocol IPv4-Only VRF to a Multiprotocol VRF Configuration, page 13](#)

## Configuring a VRF for IPv4 and IPv6 MPLS VPNs

Perform the following task to configure a VRF for IPv4 and IPv6 MPLS VPNs. When you configure a VRF for both IPv4 and IPv6 VPNs (a multiprotocol VRF), you can choose to configure route-target policies that apply to all address families in the VRF or you can configure route-target policies that apply to individual address families in the VRF.

The following task shows how to configure a VRF that has that has route-target policies defined for IPv4 and IPv6 VPNs in separate VRF address families.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** {**ipv4** | **ipv6**}
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **exit-address-family**
8. **address-family** {**ipv4** | **ipv6**}

9. **route-target** {import | export | both} *route-target-ext-community*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>vrf definition</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# vrf definition vrf1  | Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name of the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1          | Creates routing and forwarding tables for a VRF. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument specifies to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats: <ul style="list-style-type: none"> <li>16-bit autonomous system number (ASN): your 32-bit number<br/>For example, 101:3.</li> <li>32-bit IP address: your 16-bit number<br/>For example, 192.168.122.15:1.</li> </ul> </li> </ul> |
| Step 5 | <b>address-family</b> {ipv4   ipv6}<br><br><b>Example:</b><br>Router(config-vrf) address-family ipv4 | Enters VRF address family configuration mode to specify an address family for a VRF. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies an IPv4 address family for a VRF.</li> <li>The <b>ipv6</b> keyword specifies an IPv6 address family for a VRF.</li> </ul>                                                                                                                                                                                                                           |

|         | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf-af)# route-target both 100:2</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword specifies to import routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword specifies to export routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword specifies to import both import and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul>                                                                                  |
| Step 7  | <pre>exit-address-family</pre> <p><b>Example:</b><br/>Router(config-vrf-af)# exit-address-family</p>                                                  | Exits from VRF address family configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 8  | <pre>address-family {ipv4   ipv6}</pre> <p><b>Example:</b><br/>Router(config-vrf) address-family ipv6</p>                                             | <p>Enters VRF address family configuration mode to specify an address family for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies an IPv4 address family for a VRF.</li> <li>The <b>ipv6</b> keyword specifies an IPv6 address family for a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 9  | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf-af)# route-target both 100:3</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword specifies to import routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword specifies to export routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword specifies to import both import and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> <p>Enter the <b>route-target</b> command one time for each target community.</p> |
| Step 10 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-vrf-af)# end</p>                                                                                  | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Associating a Multiprotocol VRF with an Interface

Perform the following task to associate a multiprotocol VRF with an interface. Associating the VRF with an interface activates the VRF.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **vrf forwarding** *vrf-name*
5. **ip address** *ip-address mask* [**secondary**]
6. **ipv6 address** {*ipv6-address/prefix-length* | *prefix-name sub-bits/prefix-length*}
7. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                               | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 0/1                                                 | Configures an interface type and enters interface configuration mode.<br><ul style="list-style-type: none"><li>• The <b>type</b> argument identifies the type of interface to be configured.</li><li>• The <b>number</b> argument identifies the port, connector, or interface card number.</li></ul>                                                                                                                             |
| Step 4 | <b>vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# vrf forwarding vrf1                                               | Associates a VRF with an interface or subinterface.<br><ul style="list-style-type: none"><li>• The <i>vrf-name</i> argument is the name of the VRF.</li></ul>                                                                                                                                                                                                                                                                     |
| Step 5 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.24.24.24<br>255.255.255.255 | Sets a primary or secondary IP address for an interface.<br><ul style="list-style-type: none"><li>• The <i>ip-address</i> argument is the IP address.</li><li>• The <i>mask</i> argument is the mask of the associated IP subnet.</li><li>• The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li></ul> |

|        | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>ipv6 address</b> { <i>ipv6-address/prefix-length</i>   <i>prefix-name sub-bits/prefix-length</i> }<br><br><b>Example:</b><br>Router(config-if)# ipv6 address<br>2001:0DB8:0300:0201::/64 | Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface. <ul style="list-style-type: none"> <li>The <i>ipv6-address</i> argument is the IPv6 address to be used.</li> <li>The <i>prefix-length</i> argument is the length of the IPv6 prefix, which is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.</li> <li>The <i>prefix-name</i> argument is a general prefix that specifies the leading bits of the network to be configured on the interface.</li> <li>The <i>sub-bits</i> argument is the subprefix bits and host bits of the address to be concatenated with the prefixes provided by the general prefix specified with the <i>prefix-name</i> argument.</li> </ul> <p>The <i>sub-bits</i> argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.</p> |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-if) end                                                                                                                                  | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

## Verifying the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs Configuration

Perform the following task to verify the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature configuration, that is, to show that the VRF configuration is upgraded to a multi-AF multiprotocol VRF.

### SUMMARY STEPS

1. **enable**
2. **show running-config vrf** [*vrf-name*]
3. **show vrf**
4. **show vrf detail** [*vrf-name*]
5. **exit**

### DETAILED STEPS

#### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password, if prompted. For example:

```
Router> enable
Router#
```

**Step 2** **show running-config vrf** [*vrf-name*]

Use this command to verify that the upgrade to a multi-AF multiprotocol VRF configuration was successful. The following is sample command output before the upgrade to a multi-AF multiprotocol VRF:

```
Router# show running-config vrf vpn2

Building configuration...

Current configuration : 604 bytes
ip vrf vpn2
  rd 1:1
  route-target both 1:1
!
!
interface Loopback1
  ip vrf forwarding vpn2
  ip address 10.43.43.43 255.255.255.255
!
```

The following is sample command output after you upgrade to a multi-AF multiprotocol VRF with common policies for all address families:

```
Router# show running-config vrf vpn1

Building configuration...

Current configuration : 604 bytes
vrf definition vpn1
  rd 1:1
  route-target both 1:1
!
  address-family ipv4
  exit-address-family
!
!
interface Loopback1
  ip vrf forwarding vpn1
  ip address 10.43.43.43 255.255.255.255
!
```

This configuration contains the **vrf definition** command. The **vrf definition** command replaces the **ip vrf** command in the multi-AF multiprotocol VRF configuration.

**Step 3** **show vrf**

Use this command to verify that the upgrade to a multi-AF multiprotocol VRF configuration was successful. The **show vrf** command replaces the **show ip vrf** command when a VRF configuration is updated to a multi-AF multiprotocol VRF configuration. The **show vrf** command displays the protocols defined for a VRF. The following command shows sample output after you upgrade a single-protocol VRF configuration to a multi-AF multiprotocol VRF configuration:

```
Router# show vrf vpn1
```

| Name | Default RD | Protocols | Interfaces |
|------|------------|-----------|------------|
| vpn1 | 1:1        | ipv4      | Lo1/0      |

The following is sample output from the **show ip vrf vp1** command. Compare this to the output of the **show vrf vp1** command. The protocols under the VRF are not displayed.

```
Router# show ip vrf vrf1
```

| Name | Default RD | Interface |
|------|------------|-----------|
| vp1  | 1:1        | Loopback1 |

The following is sample output from the **show vrf** command for multiprotocol VRFs, one of which contains both IPv4 and IPv6 protocols:

```
Router# show vrf
```

| Name | Default RD | Protocols  | Interfaces     |
|------|------------|------------|----------------|
| vp1  | 1:1        | ipv4       | Lo1/0          |
| vp2  | 100:3      | ipv4       | Lo23 AT3/0/0.1 |
| vp4  | 100:2      | ipv4, ipv6 |                |

#### Step 4 **show vrf detail [vrf-name]**

Use this command to display all characteristics of the defined VRF to verify that the configuration is as you expected. For example, if your VRF configuration for VRF vp1 is as follows:

```
vrf definition vp1
 route-target both 100:1
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 route-target both 100:1
 route-target import 100:3
 exit-address-family
```

This command would display the following:

```
Router# show vrf detail vp1
```

```
VRF vp1 (VRF Id = 3); default RD <not set>; default VPNID <not set>
  No interfaces
Address family ipv4 (Table ID = 3 (0x3)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1

  Import VPN route-target communities
    RT:100:1          RT:100:2

  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 (Table ID = 503316483 (0x1E000003)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1

  Import VPN route-target communities
    RT:100:1          RT:100:3

  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

**Step 5**    **exit**

Use this command to exit to user EXEC mode. For example:

```
Router# exit
Router>
```

## Migrating from a Single-Protocol IPv4-Only VRF to a Multiprotocol VRF Configuration

Perform the following task to force migration from a single-protocol IPv4-only VRF to a multiprotocol VRF configuration.

The multiprotocol VRF configuration allows you to define multiple address families under the same VRF. A given VRF, identified by its name and a set of policies, can apply to both an IPv4 VPN and an IPv6 VPN at the same time. This VRF can be activated on a given interface, even though the routing and forwarding tables are different for the IPv4 and IPv6 protocols.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf upgrade-cli multi-af-mode {common-policies | non-common-policies} [vrf vrf-name]**
4. **exit**
5. **show running-config vrf vrf-name**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                          |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                  |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                  |



|        | Command or Action                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <p><b>vrf upgrade-cli multi-af-mode</b> {<b>common-policies</b>   <b>non-common-policies</b>} [<b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b><br/> Router(config)# vrf upgrade-cli multi-af-mode common-policies vrf vpn4</p> | <p>Upgrades a VRF instance or all VRFs configured on the router to support multiple address families under the same VRF.</p> <ul style="list-style-type: none"> <li>The <b>multi-af-mode</b> keyword specifies an upgrade of a single-protocol VRF or all VRFs to a multiprotocol VRF that supports multi-AFs configuration.</li> <li>The <b>common-policies</b> keyword specifies to copy the route-target policies to the common part of the VRF configuration so that the policies apply to all address families configured in the multi-AF VRF.</li> <li>The <b>non-common-policies</b> keyword specifies to copy the route-target policies to the IPv4 address family part of the VRF configuration so that the policies apply only to IPv4.</li> <li>The <b>vrf</b> keyword specifies a VRF for the upgrade to a multi-AF VRF configuration.</li> <li>The <i>vrf-name</i> argument is the name of the single-protocol VRF to upgrade to a multi-AF VRF configuration.</li> </ul> |
| Step 4 | <p><b>exit</b></p> <p><b>Example:</b><br/> Router(config)# exit</p>                                                                                                                                                               | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 5 | <p><b>show running-config vrf</b> [<i>vrf-name</i>]</p> <p><b>Example:</b><br/> Router# show running-config vrf vpn4</p>                                                                                                          | <p>Displays the subset of the running configuration of a router that is linked to a specific VRF instance or to all VRFs configured on the router.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name of the VRF of which you want to display the configuration.</li> </ul> <p><b>Note</b> The Cisco IOS image that supports the multiprotocol VRF commands might not support the <b>show running-config vrf</b> command. You can use the <b>show running-config</b> command instead.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Configuration Examples for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

The following examples show how to use the VRF CLI provided by the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature to migrate from a single-protocol VRF to a multiprotocol VRF configuration:

- [Configuring a VRF for IPv4 and IPv6 VPNs: Example, page 15](#)
- [Associating a Multiprotocol VRF with an Interface: Example, page 15](#)
- [Migrating from a Single-Protocol IPv4-Only VRF Configuration to a Multiprotocol VRF Configuration: Example, page 16](#)

## Configuring a VRF for IPv4 and IPv6 VPNs: Example

The following example shows how to configure a VRF for IPv4 and IPv6 VPNs:

```
configure terminal
!
vrf definition vrf1
  rd 100:1
!
  address-family ipv4
    route-target both 100:2
  exit-address-family
!
  address-family ipv6
    route-target both 100:3
  exit-address-family
```

In this example, noncommon policies are defined in the address-family configuration.

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
configure terminal
!
vrf definition vrf2
  rd 200:1
  route-target both 200:2
!
  address-family ipv4
  exit-address-family
!
  address-family ipv6
  exit-address-family
end
```

## Associating a Multiprotocol VRF with an Interface: Example

The following example shows how to associate a multiprotocol VRF with an interface:

```
configure terminal
!
interface Ethernet 0/1
  vrf forwarding vrf1
  ip address 10.24.24.24 255.255.255.255
  ipv6 address 2001:0DB8:0300:0201::/64
end
```

## Migrating from a Single-Protocol IPv4-Only VRF Configuration to a Multiprotocol VRF Configuration: Example

This section contains examples that show how to migrate from a single-protocol IPv4-only VRF to a multiprotocol VRF configuration.

This example shows a single-protocol IPv4-only VRF before the Cisco IOS VRF CLI for IPv4 and IPv6 is entered on the router:

```
ip vrf vrf1
  rd 1:1
  route-target both 1:1

interface Loopback1
  ip vrf forwarding V1
  ip address 10.3.3.3 255.255.255.255
```

This example shows how to force the migration of the single-protocol VRF vrf1 to a multiprotocol VRF configuration:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
!
Router(config)# vrf upgrade-cli multi-af-mode common-policies vrf vrf1
```

```
You are about to upgrade to the multi-AF VRF syntax commands.
You will loose any IPv6 address configured on interfaces
belonging to upgraded VRFs.
Are you sure ? [yes]: yes
```

```
Number of VRFs upgraded: 1
```

```
Router(config)# exit
```

This example shows the multiprotocol VRF configuration after the forced migration:

```
vrf definition vrf1
  rd 1:1
  route-target both 1:1
  !
  address-family ipv4
  exit-address-family
  !

interface Loopback1
  vrf forwarding V1
  ip address 10.3.3.3 255.255.255.255
```

The following is another example of a multi-AF multiprotocol VRF configuration:

```
vrf definition vrf2
  rd 100:1
  address family ipv6
  route-target both 200:1
  exit-address-family
  !
ip vrf vrf1
  rd 200:1
  route-target both 200:1
  !
interface Ethernet0/0
  vrf forwarding vrf2
```

```
ip address 10.50.1.2 255.255.255.0
ipv6 address 2001:0DB8:0:1::/64
!
interface Ethernet0/1
 ip vrf forwarding vrf1
 ip address 10.60.1.2 255.255.255.0
 ipv6 address 2001:0DB8:1:1::/64
```

In this example, all addresses (IPv4 and IPv6) defined for interface Ethernet0/0 are in VRF vrf2. For the interface Ethernet0/1, the IPv4 address is defined in VRF vrf1 but the IPv6 address is in the global IPv6 routing table.

## Additional References

The following sections provide references related to the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature.

## Related Documents

| Related Topic                               | Document Title                                                              |
|---------------------------------------------|-----------------------------------------------------------------------------|
| MPLS                                        | <a href="#">MPLS Product Literature</a>                                     |
| Commands for configuring MPLS and MPLS VPNs | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>   |
| Configuration tasks for MPLS and MPLS VPNs  | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                              |
|----------|----------------------------------------------------|
| RFC 1771 | <i>A Border Gateway Protocol 4 (BGP-4)</i>         |
| RFC 4364 | <i>BGP MPLS/IP Virtual Private Networks (VPNs)</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **show vrf**
- **vrf definition**
- **vrf forwarding**
- **vrf upgrade-cli**

# Feature Information for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs

| Feature Name                            | Releases                   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs | 12.2(33)SRB<br>12.2(33)SXI | <p>This document describes how to configure a multiprotocol Virtual Private Network (VPN) routing and forwarding (VRF) instance for IPv4 and IPv6 VPNs and describes how to upgrade your existing single-protocol IPv4-only VRF to a multiprotocol VRF configuration.</p> <p>The MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs feature introduces Cisco IOS command-line interface (CLI) commands that allow you to enable an IPv4 and IPv6 VPN in the same Multiprotocol Label Switching (MPLS) VRF instance and to simplify the migration from a single-protocol VRF configuration to a multiprotocol VRF configuration.</p> <p>In 12.2(33)SRB, this feature was introduced on the Cisco 7600 router.</p> <p>In 12.2(33)SXI, this feature was integrated into a Cisco IOS 12.2SXI release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">VRF Concepts Similar for IPv4 and IPv6 MPLS VPNs, page 2</a></li> <li>• <a href="#">Single-Protocol VRF to Multiprotocol VRF Migration, page 3</a></li> <li>• <a href="#">Multiprotocol VRF Configurations Characteristics and Examples, page 4</a></li> <li>• <a href="#">Configuring a VRF for IPv4 and IPv6 MPLS VPNs, page 6</a></li> <li>• <a href="#">Associating a Multiprotocol VRF with an Interface, page 9</a></li> </ul> |

**Table 1**      *Feature Information for MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs (continued)*

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <ul style="list-style-type: none"><li>• <a href="#">Verifying the MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs Configuration, page 10</a></li><li>• <a href="#">Migrating from a Single-Protocol IPv4-Only VRF to a Multiprotocol VRF Configuration, page 13</a></li></ul> <p>The following commands were introduced or modified: <b>show vrf</b>, <b>vrf definition</b>, <b>vrf forwarding</b>, <b>vrf upgrade-cli</b>.</p> |

# Glossary

**6PE**—IPv6 provider edge router or a Multiprotocol Label Switching (MPLS) label switch router (LSR) edge router using IPv6.

**6VPE**—IPv6 Virtual Private Network (VPN) provider edge router.

**AF**—address family. Set of related communication protocols in which all members use a common addressing mechanism to identify endpoints. Also called protocol family.

**AFI**—Address Family Identifier. Carries the identity of the network-layer protocol that is associated with the network address.

**BGP**—Border Gateway Protocol. A routing protocol used between autonomous systems. It is the routing protocol that makes the internet work. BGP is a distance-vector routing protocol that carries connectivity information and an additional set of BGP attributes. These attributes allow for a set of policies for deciding the best route to use to reach a given destination. BGP is defined by RFC 1771.

**CE**—customer edge router. A service provider router that connects to Virtual Private Network (VPN) customer sites.

**FIB**—Forwarding Information Base. Database that stores information about switching of data packets. A FIB is based on information in the Routing Information Base (RIB). It is the optimal set of selected routes that are installed in the line cards for forwarding.

**HA**—high availability. High availability is defined as the continuous operation of systems. For a system to be available, all components—including application and database servers, storage devices, and the end-to-end network—need to provide continuous service.

**IP**—Internet Protocol. Network-layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security.

**IPv4**—IP Version 4. Network layer for the TCP/IP protocol suite. IPv4 is a connectionless, best-effort packet switching protocol.

**IPv6**—IP Version 6. Replacement for IPv4. IPv6 is a next-generation IP protocol. IPv6 is backward compatible with and designed to fix the shortcomings of IPv4, such as data security and maximum number of user addresses. IPv6 increases the address space from 32 to 128 bits, providing for an unlimited number of networks and systems. It also supports quality of service (QoS) parameters for real-time audio and video.

**MFI**—MPLS Forwarding Infrastructure. In the Cisco MPLS subsystem, the data structure for storing information about incoming and outgoing labels and associated equivalent packets suitable for labeling.

**MPLS**—Multiprotocol Label Switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**PE**—provider edge router. A router that is part of a service provider's network and that is connected to a customer edge (CE) router. The PE router function is a combination of an MLS edge label switch router (LSR) function with some additional functions to support Virtual Private Networks (VPNs).

**RD (IPv4)**—route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 (VPNv4) prefix.

**RD (IPv6)**—route distinguisher. A 64-bit value that is prepended to an IPv6 prefix to create a globally unique VPN-IPv6 address.



**RIB**—Routing Information Base. The set of all available routes from which to choose the Forwarding Information Base (FIB). The RIB essentially contains all routes available for selection. It is the sum of all routes learned by dynamic routing protocols, all directly attached networks (that is—networks to which a given router has interfaces connected), and any additional configured routes, such as static routes.

**RT**—route target. Extended community attribute used to identify the Virtual Private Network (VPN) routing and forwarding (VRF) routing table into which a prefix is to be imported.

**VPN**—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

**VRF**—Virtual Private Network (VPN) routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

**VRF table**—A routing and a forwarding table associated to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. This is a customer-specific table, enabling the provider edge (PE) router to maintain independent routing states for each customer.

---

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

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

© 2006–2008 Cisco Systems, Inc. All rights reserved.



# MPLS VPN—BGP Local Convergence

---

**First Published: December 31, 2007**

**Last Updated: October 2, 2009**

The MPLS VPN—BGP Local Convergence feature reduces the downtime of a provider edge (PE) to customer edge (CE) link failure. It does so by rerouting PE-egress traffic onto a backup path to the CE before BGP has re-converged.

The MPLS VPN—BGP Local Convergence feature is also referred to as “local protection”.

Note that the MPLS VPN—BGP Local Convergence feature only affects traffic exiting the VPN. Therefore, it cannot fully protect traffic end-to-end by itself.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN—BGP Local Convergence”](#) section on page 13.

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

## Contents

- [Prerequisites for MPLS VPN—BGP Local Convergence, page 2](#)
- [Restrictions for MPLS VPN—BGP Local Convergence, page 2](#)
- [Information About MPLS VPN—BGP Local Convergence, page 3](#)
- [How to Enable MPLS VPN—BGP Local Convergence, page 5](#)
- [Configuration Examples for MPLS VPN—BGP Local Convergence, page 8](#)
- [Additional References, page 12](#)
- [Feature Information for MPLS VPN—BGP Local Convergence, page 13](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS VPN—BGP Local Convergence

- Before this form of link protection can be enabled, the customer site must be connected to the provider site by more than one path.
- Both the main forwarding path and the redundant backup path must have been installed within BGP, and BGP must support lossless switchover between operational paths.

**Note**

Any routing protocol can be used between the PE and CE as long as the path is redistributed into BGP. That includes: eBGP, RIP, EIGRP, IS-IS, OSPF, and static routing. Any next-hop core tunneling technology that is supported by BGP is also supported for protection, including MPLS, IP/L2TPv3, and IP/GRE. Enabling a Carrier's Carrier (CsC) protocol between the PE and CE is also supported. Inter-AS option A (back-to-back VRF) is supported because it is essentially the same as performing the PE-CE link protection in both AS's. However, inter-AS options B and C protection are not supported at this time.

- All Provider Edge routers that are serving as backup to the link must have assigned a unique Route Distinguisher to each Virtual Routing and Forwarding table involved with the link to ensure that the route reflectors advertise all available paths.
- Although not required, it is recommended that the backup PE (shown as “PE2” in [Figure 2](#)) also be running the IOS version that is running on the PE (“PE1”) whose link with the CE will be protected; that is, Cisco IOS Release 12.2(33)SRC, Cisco IOS Release 12.2(33)SB, Cisco IOS Release 15.0(1)M or a more recent version of those products.

## Restrictions for MPLS VPN—BGP Local Convergence

- This feature only affects traffic exiting the VPN. Therefore, it cannot fully protect traffic end-to-end by itself.
- Configuration of this feature is not allowed in IPv6.
- Local protection is not applicable with VRF-lite. Although configuration of both features together is not blocked, protection does not occur.
- This link protection cannot be initiated *during* an HA stateful switchover (SSO). But links already configured with this protection *before* the switchover begins will remain protected after the switchover.
- When performing an ISSU downgrade from an image that does include this link protection to an image that does not support this feature, active protection will be halted when BGP routes are refreshed.

# Information About MPLS VPN—BGP Local Convergence

To configure the MPLS VPN—BGP Local Convergence feature, you should understand the following concepts:

- [How Link Failures Are Handled with BGP, page 3](#)
- [How Links Are Handled with the MPLS VPN—BGP Local Convergence Feature, page 3](#)
- [How Link Failures Are Detected, page 4](#)

## How Link Failures Are Handled with BGP

Within a Layer 3 VPN network, the failure of a PE-CE link can cause a loss of connectivity (LoC) to a customer site, which is detrimental to time-sensitive applications. Several factors contribute to the duration of such an outage:

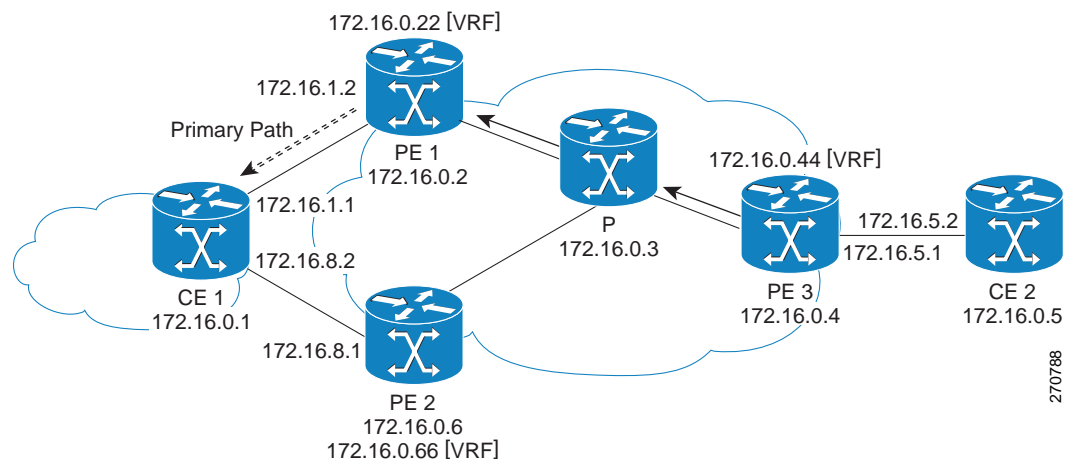
- The time to detect the failure
- The programming of the forwarding
- The convergence of BGP (In large networks, the restored traffic arrival time at its destination varies according to the prefix.)

When BGP detects a PE-CE link failure, it removes all of the BGP paths through the failing link. BGP runs the bestpath algorithm on the affected prefixes and selects alternate paths for each prefix. These new paths (which typically include a remote PE) are installed into forwarding. The local labels are removed and BGP withdrawals are sent to all BGP neighbors. As each BGP neighbor receives the withdrawal messages (typically indirectly using route-reflectors), the bestpath algorithm is called and the prefixes are switched to an alternate path. Only then is connectivity restored.

## How Links Are Handled with the MPLS VPN—BGP Local Convergence Feature

The MPLS VPN—BGP Local Convergence feature requires that the prefixes to be protected on a PE-CE link have at least one backup path that does not include that link. (See Figure 1.) The customer site must have backup paths to the provider site.

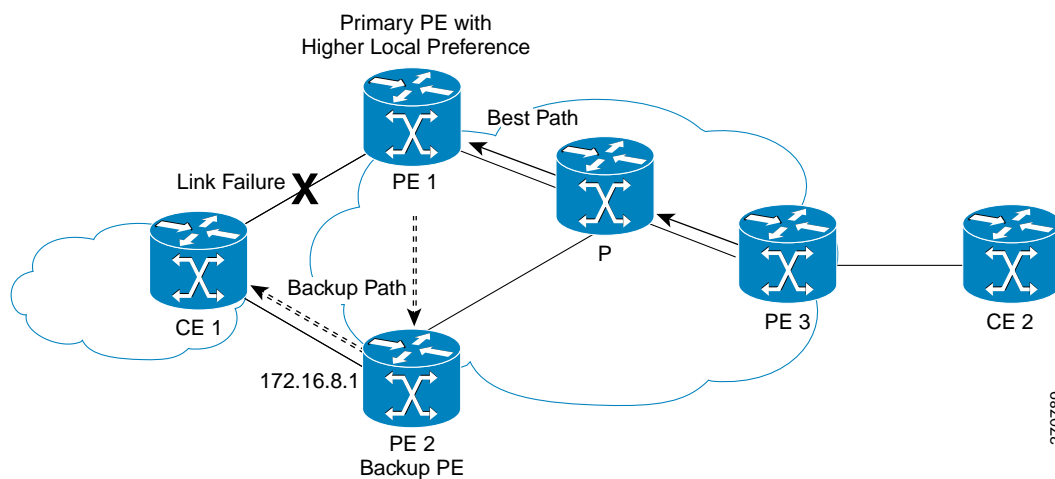
**Figure 1** *Figure 1 Network Configured with Primary and Backup Paths*



The MPLS VPN—BGP Local Convergence feature reduces LoC time by sending the broken link's traffic over a backup path (as shown in Figure 2) instead of waiting for total network convergence. The local label is maintained for 5 minutes while prefixes switch from the failing local path to the backup path. Because the label is not freed as had been the usual practice, forwarding continues to take place.

The bestpath algorithm selects the backup path. Thus, the local label has been applied in place of the failed BGP bestpath label (which is sometimes called "label swapping"). Traffic is restored locally while the network propagation of the BGP withdrawal messages takes place. Eventually, the egress PE router converges and bypasses the local repair.

**Figure 2** *Figure 2 Network Using the Backup Path After a PE-CE Link Failure on the Primary Path*



#### Note

After the 5-minute label preservation, the local labels are freed. Any BGP prefix that is remote and is not part of a Carrier Supporting Carrier network does not have a local label and is removed. The delay in local label deletion does not modify normal BGP addition and deletion of BGP paths. Rather, BGP re-programs the new backup bestpath into forwarding as usual.

## How Link Failures Are Detected

Local protection relies on BGP being notified of the interface failure. Detection can occur using either the interface drivers or the routing tables. If an interface or route goes down, the corresponding path in the routing table is removed and BGP will be notified using the routing APIs.

However, when the routing table cannot detect the failure (as when a Layer 2 switch goes down), BGP determines that a neighbor is down through use of its hold-down timer. However, that determination can be extremely slow because of the 3-minute default for BGP session time-out.

You can reduce the detection delay by either reducing the BGP session time-out interval (as described in the [Configuring Internal BGP Features](#) document) or by enabling the Bidirectional Forwarding Detection protocol within eBGP between the PE and CE. For complete instructions to enable BFD, see the [Bidirectional Forwarding Detection](#) document.

# How to Enable MPLS VPN—BGP Local Convergence

This section contains the following information:

- [Configuring MPLS VPN—BGP Local Convergence with IPv4, page 5](#)
- [Configuring MPLS VPN—BGP Local Convergence with IPv6, page 6](#)
- [Troubleshooting Tips, page 8](#)

## Configuring MPLS VPN—BGP Local Convergence with IPv4

Perform the following steps to configure MPLS VPN—BGP Local Convergence for IPv4 MPLS VPNs.

### Prerequisite

Ensure that the CE is already connected to the PE by a minimum of two paths.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd** (conditional)
5. **protection local-prefixes**
6. **show ip vrf detail**

### DETAILED STEPS

|        | Command or Action                                                                   | Purpose                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                              | Enables privileged EXEC mode. Enter your password if prompted.                                                                                                                                                                                                                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal      | Enters global configuration mode.                                                                                                                                                                                                                                                  |
| Step 3 | <b>ip vrf <i>vrf-name</i></b><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1 | Enters VRF configuration mode. If no VRF routing table and Cisco Express Forwarding (CEF) table had been previously created for this named VRF, then this command also creates them, giving both tables the specified <i>vrf-name</i> (in this example, the name is <i>vpn1</i> ). |

|        | Command or Action                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# <b>rd</b> 100:3              | (Optional). If no route distinguisher had been previously established for the named VRF, then it is necessary to enter this command.<br><br>The <i>route-distinguisher</i> value can be either an: <ul style="list-style-type: none"> <li>autonomous system number followed by a colon and an arbitrary number (for example, 100:3)</li> <li>or</li> <li>IP address followed by a colon and an arbitrary number (for example, 192.168.122.15:1).</li> </ul> |
| Step 5 | <b>protection local-prefixes</b><br><br><b>Example:</b><br>Router(config-vrf)# <b>protection local-prefixes</b> | Allows a pre-configured backup path to carry traffic if the PE-CE link breaks by preserving the local prefixes while BGP reconverges.                                                                                                                                                                                                                                                                                                                       |
| Step 6 | <b>show ip vrf detail</b><br><br><b>Example:</b><br>Router(config-vrf)# <b>show ip vrf detail</b>               | (Optional) Verifies that MPLS VPN—BGP Local Convergence has been configured. (See Examples.)                                                                                                                                                                                                                                                                                                                                                                |

## Configuring MPLS VPN—BGP Local Convergence with IPv6

Perform the following steps to configure MPLS VPN—BGP Local Convergence for IPv6 MPLS VPNs.

### Prerequisite

Ensure that the CE is already connected to the PE by a minimum of two paths.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** (optional)
5. **address-family** [ipv4 | ipv6]
6. **protection local-prefixes**
7. **show ip vrf detail**

## DETAILED STEPS

|        | Command or Action                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                      | Enables privileged EXEC mode. Enter your password if prompted.                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 3 | <b>vrf definition vrf-name</b><br><br><b>Example:</b><br>Router(config)# vrf definition vrf2                | Enters VRF definition configuration mode. If no VRF routing table and Cisco Express Forwarding (CEF) table had been previously created for this named VRF, then this command also creates them, giving both tables the specified <i>vrf-name</i> (in this example, the name is <i>vrf2</i> ).                                                                                                                                                         |
| Step 4 | <b>rd route-distinguisher</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:3                        | (Optional) If no route distinguisher had been previously established for the named VRF, it is necessary to enter this command.<br><br>The <i>route-distinguisher</i> value can be either an: <ul style="list-style-type: none"> <li>autonomous system number followed by a colon and an arbitrary number (for example, 100:3)</li> <li>or</li> <li>IP address followed by a colon and an arbitrary number (for example, 192.168.122.15:1).</li> </ul> |
| Step 5 | <b>address-family [ ipv4   ipv6 ]</b><br><br><b>Example:</b><br>Router(config-vrf)# address-family ipv6     | Enters address family configuration mode and specifies the IPv4 or IPv6 protocol.                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | <b>protection local-prefixes</b><br><br><b>Example:</b><br>Router(config-vrf-af)# protection local-prefixes | Allows a pre-configured backup path to carry traffic if the PE-CE link breaks by preserving the local prefixes while BGP reconverges.                                                                                                                                                                                                                                                                                                                 |
| Step 7 | <b>show ip vrf detail</b><br><br><b>Example:</b><br>Router(config-vrf)# show ip vrf detail                  | (Optional) Verifies that MPLS VPN—BGP Local Convergence has been configured. (See Examples.)                                                                                                                                                                                                                                                                                                                                                          |



## Examples

To verify that local link protection has been enabled, enter the VRF detail command **show ip vrf detail**. If the protection is enabled, the status message “Local prefix protection enabled” will be shown in the display:

```
Router# show ip vrf detail
VRF vpn1 (VRF Id = 1); default RD 100:1; default VPNID <not set>
  Interfaces:
    AT1/0/1.1
VRF Table ID = 1
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1          RT:100:2
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
    Local prefix protection enabled
```

## Troubleshooting Tips

- Ensure that a minimum of two paths are present for the protected prefix *w.x.y.z* in BGP in steady state condition on the PE. The path using the protected PE should be the BGP best-path before failover occurs. To view the configuration, enter the command **show ip bgp vpnv4 vrf vpn w.x.y.z**.
- Ensure that local protection has been enabled in the protected PE by entering the **show ip vrf detail** command as shown in the “Examples” section on page 8.
- When route reflectors exist in the topology, ensure that each VRF has a unique route distinguisher.

# Configuration Examples for MPLS VPN—BGP Local Convergence

The following examples show how MPLS VPN—BGP Local Convergence can prevent traffic loss after a link failure. You can display a detailed view of local link protection before, during, and after BGP convergence by using the **show bgp vpnv4** and **show mpls forwarding-table vrf** commands as shown in the following 3-stage example.



### Note

The **show bgp vpnv4 unicast** command is equivalent to the **show ip bgp vpnv4** command that existed in prior releases of Cisco IOS.

### Example 1: Before the Link Failure

Both a primary path and a backup path have been configured:

```
PE1# show bgp vpnv4 unicast all 172.16.0.1
BGP routing table entry for 100:1:172.16.0.1/32, version 2
Paths: (2 available, best #2, table v1)
Flag: 0x820
  Advertised to update-groups:
    1
    100, imported path from 100:2:172.16.0.1/32
```

```

172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
  Origin incomplete, metric 0, localpref 100, valid, internal
  Extended Community: RT:100:0
  Originator: 172.16.0.6, Cluster list: 172.16.0.7
  mpls labels in/out 16/17
100
172.16.1.1 from 172.16.1.1 (172.16.0.1)
  Origin incomplete, metric 0, localpref 100, valid, external, best
  Extended Community: RT:100:0
  mpls labels in/out 16/nolabel
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
Flag: 0x820
  Not advertised to any peer
100
172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
  Origin incomplete, metric 0, localpref 100, valid, internal, best
  Extended Community: RT:100:0
  Originator: 172.16.0.6, Cluster list: 172.16.0.7
  mpls labels in/out nolabel/17

```

Label information for both paths can be displayed:

```

PE1# show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 100:1 (v1)
  172.16.0.1/32   172.16.0.6        16/17
                   172.16.1.1        16/nolabel
  172.16.0.5/32   172.16.0.4        nolabel/23
  172.16.0.22/32  0.0.0.0           17/nolabel(v1)
  172.16.0.44/32  172.16.0.4        nolabel/24
  172.16.0.66/32  172.16.0.6        nolabel/21
  172.16.1.0/24   172.16.1.1        18/nolabel
                   0.0.0.0           18/nolabel(v1)
  172.16.5.0/24   172.16.0.4        nolabel/25
  172.16.8.0/24   172.16.0.6        19/23
                   172.16.1.1        19/nolabel
Route Distinguisher: 100:2
  172.16.0.1/32   172.16.0.6        nolabel/17
  172.16.0.66/32  172.16.0.6        nolabel/21
  172.16.8.0/24   172.16.0.6        nolabel/23

```

The PE1 (see [Figure 1 on page 3](#)) forwarding table contains BGP bestpath information:

```

PE1# show mpls forwarding-table vrf v1 172.16.0.1 detail
Local   Outgoing Prefix      Bytes Label  Outgoing  Next Hop
Label   Label    or Tunnel Id  Switched     interface
16      No Label  172.16.0.1/32[v] 570          Et0/0     172.16.1.1
MAC/Encaps=14/14, MRU=1504, Label Stack{}
AABBCC000B00AABBCC000C000800
VPN route: v1
No output feature configured

PE1#

```

**Example 2: After the Link Failure and Before BGP Convergence**

After the link failure on only one path, the backup path remains available (see [Figure 2 on page 4](#)):

```

PE1# show bgp vpnv4 unicast all 172.16.0.1
BGP routing table entry for 100:1:172.16.0.1/32, version 19
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out 16/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17

```

The label information for the backup path label can be displayed:

```

PE1# show bgp vpnv4 unicast all labels
Network          Next Hop          In label/Out label
Route Distinguisher: 100:1 (v1)
  172.16.0.1/32   172.16.0.6         16/17
  172.16.0.5/32   172.16.0.4         nolabel/23
  172.16.0.22/32  0.0.0.0            17/nolabel(v1)
  172.16.0.44/32  172.16.0.4         nolabel/24
  172.16.0.66/32  172.16.0.6         nolabel/21
  172.16.1.0/24   172.16.0.6         nolabel/22
  172.16.5.0/24   172.16.0.4         nolabel/25
  172.16.8.0/24   172.16.0.6         19/23
Route Distinguisher: 100:2
  172.16.0.1/32   172.16.0.6         nolabel/17
  172.16.0.66/32  172.16.0.6         nolabel/21
  172.16.1.0/24   172.16.0.6         nolabel/22
  172.16.8.0/24   172.16.0.6         nolabel/23

```

The PE1 (see [Figure 1 on page 3](#)) forwarding table contains new label and next-hop information to direct traffic onto the backup path:

```

PE1# show mpls forwarding-table vrf v1 172.16.0.1 detail
Local      Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label      Label    or Tunnel Id   Switched     interface
16         17       172.16.0.1/32[V] 0             Et1/0      172.16.3.2
          MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
          AABBC000D00AABBC000C018847 0001500000011000
          VPN route: v1
          No output feature configured
PE1#

```

**Example 3: After Local Label Expiration and BGP Re-convergence**

Because the local label preservation window has expired, the replacement local label is now gone from the PE1 forwarding table information:

```
PE1# show mpls forwarding-table vrf v1 172.16.0.1 detail
Local      Outgoing  Prefix          Bytes Label  Outgoing  Next Hop
Label      Label      or Tunnel Id    Switched     interface
None       17         172.16.0.1/32[V] 0           Et1/0       172.16.3.2
          MAC/Encaps=14/22, MRU=1496, Label Stack{21 17}
          AABBC000D00AABBC000C018847 0001500000011000
          VPN route: v1
          No output feature configured
```

The new BGP information reverts to the configuration shown in [Figure 1 on page 3](#):

```
PE1# show bgp vpnv4 unicast all 172.16.0.1
BGP routing table entry for 100:1:172.16.0.1/32, version 23
Paths: (1 available, best #1, table v1)
  Not advertised to any peer
  100, imported path from 100:2:172.16.0.1/32
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17
BGP routing table entry for 100:2:172.16.0.1/32, version 9
Paths: (1 available, best #1, no table)
  Not advertised to any peer
  100
    172.16.0.6 (metric 21) from 172.16.0.7 (172.16.0.7)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:0
      Originator: 172.16.0.6, Cluster list: 172.16.0.7
      mpls labels in/out nolabel/17

PE1# show bgp vpnv4 unicast all labels
Network      Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
  172.16.0.1/32  172.16.0.6    nolabel/17
  172.16.0.5/32  172.16.0.4    nolabel/23
  172.16.0.22/32 0.0.0.0       17/nolabel(v1)
  172.16.0.44/32 172.16.0.4    nolabel/24
  172.16.0.66/32 172.16.0.6    nolabel/21
  172.16.1.0/24  172.16.0.6    nolabel/22
  172.16.5.0/24  172.16.0.4    nolabel/25
  172.16.8.0/24  172.16.0.6    nolabel/23
Route Distinguisher: 100:2
  172.16.0.1/32  172.16.0.6    nolabel/17
  172.16.0.66/32 172.16.0.6    nolabel/21
  172.16.1.0/24  172.16.0.6    nolabel/22
  172.16.8.0/24  172.16.0.6    nolabel/23

PE1#
```

# Additional References

The following sections provide references related to the MPLS VPN—BGP Local Convergence feature.

- [Related Documents, page 12](#)
- [Standards, page 12](#)
- [MIBs, page 12](#)
- [RFCs, page 12](#)
- [Technical Assistance, page 13](#)

## Related Documents

| Related Topic                                                              | Document Title                                                 |
|----------------------------------------------------------------------------|----------------------------------------------------------------|
| Configuration of VRF under the specific cases of IPv4 and IPv6 situations. | <a href="#"><i>MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs</i></a> |
| Protocol for quickly detecting failed forwarding paths.                    | <a href="#"><i>Bidirectional Forwarding Detection</i></a>      |
| BGP Configuration                                                          | <a href="#"><i>Configuring a Basic BGP Network</i></a>         |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                |
|----------|----------------------|
| RFC 2547 | <i>BGP/MPLS VPNs</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN—BGP Local Convergence

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—BGP Local Convergence

| Feature Name                   | Releases    | Feature Information                                                                                                                                                                                                                                                                                                               |
|--------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—BGP Local Convergence | 12.2(33)SRC | <p>This feature reduces the downtime of a PE-CE link failure by rerouting PE-egress traffic onto a backup path to the CE before BGP has re-converged.</p> <p>In 12.2(33)SRC, this feature was introduced on the Cisco 7200 and the Cisco 7600.</p> <p>The following command was introduced: <b>protection local-prefixes</b>.</p> |
| MPLS VPN—BGP Local Convergence | 12.2(33)SB  | <p>This feature became available on the Cisco 7300 series and the Cisco 10000 series routers.</p>                                                                                                                                                                                                                                 |
| MPLS VPN—BGP Local Convergence | 15.0(1)M    | <p>This feature was integrated in this release. The following command was introduced: <b>protection local-prefixes</b>.</p>                                                                                                                                                                                                       |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus,

Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



# MPLS VPN—Route Target Rewrite

---

**First Published: August 26, 2003**

**Last Updated: July 11, 2008**

The MPLS VPN—Route Target Rewrite feature allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Typically, Autonomous System Border Routers (ASBRs) perform the replacement of route targets at autonomous system boundaries. Route Reflectors (RRs) and provider edge (PE) routers can also perform route target replacement.

The main advantage of the MPLS VPN—Route Target Rewrite feature is that it keeps the administration of routing policy local to the autonomous system.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS VPN—Route Target Rewrite”](#) section on [page 19](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS VPN—Route Target Rewrite, page 2](#)
- [Restrictions for MPLS VPN—Route Target Rewrite, page 2](#)
- [Information About MPLS VPN—Route Target Rewrite, page 2](#)
- [How to Configure MPLS VPN—Route Target Rewrite, page 4](#)
- [Configuration Examples for MPLS VPN—Route Target Rewrite, page 15](#)
- [Additional References, page 17](#)



---

**Americas Headquarters:**

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



- [Command Reference, page 18](#)
- [Feature Information for MPLS VPN—Route Target Rewrite, page 19](#)
- [Glossary, page 20](#)

## Prerequisites for MPLS VPN—Route Target Rewrite

The MPLS VPN—Route Target Rewrite feature requires the following:

- You should know how to configure Multiprotocol Virtual Private Networks (MPLS VPNs).
- You need to configure your network to support interautonomous systems with different route target (RT) values in each autonomous system.
- You need to identify the RT replacement policy and target router for each autonomous system.

## Restrictions for MPLS VPN—Route Target Rewrite

You can apply multiple replacement rules using the route-map continue clause. The MPLS VPN—Route Target Rewrite feature does not support the continue clause on outbound route maps.

## Information About MPLS VPN—Route Target Rewrite

To configure the MPLS VPN—Route Target Rewrite feature, you need to understand the following concepts:

- [Route Target Replacement Policy, page 2](#)
- [Route Maps and Route Target Replacement, page 4](#)

## Route Target Replacement Policy

Routing policies for a peer include all configurations that may impact inbound or outbound routing table updates. The MPLS VPN—Route Target Rewrite feature can influence routing table updates by allowing the replacement of route targets on inbound and outbound BGP updates. Route targets are carried as extended community attributes in BGP Virtual Private Network IP Version 4 (VPNv4) updates. Route target extended community attributes are used to identify a set of sites and VPN routing and forwarding (VRF) instances that can receive routes with a configured route target.

In general, ASBRs perform route target replacement at autonomous system borders when the ASBRs exchange VPNv4 prefixes. You can also configure the MPLS VPN—Route Target Rewrite feature on PE routers and RR routers.

[Figure 1](#) shows an example of route target replacement on ASBRs in an MPLS VPN interautonomous system topology. This example includes the following configurations:

- PE1 is configured to import and export RT 100:1 for VRF VPN1.
- PE2 is configured to import and export RT 200:1 for VRF VPN2.
- ASBR1 is configured to rewrite all inbound VPNv4 prefixes with RT 200:1 to RT 100:1.
- ASBR2 is configured to rewrite all inbound VPNv4 prefixes with RT 100:1 to RT 200:1.

**Figure 1** *Route Target Replacement on ASBRs in an MPLS VPN Interautonomous System Topology*

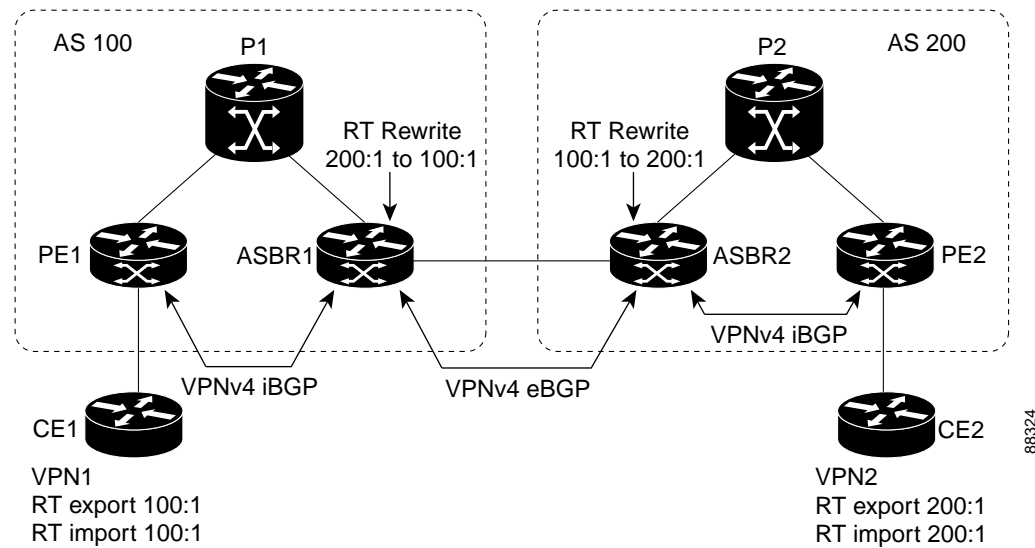
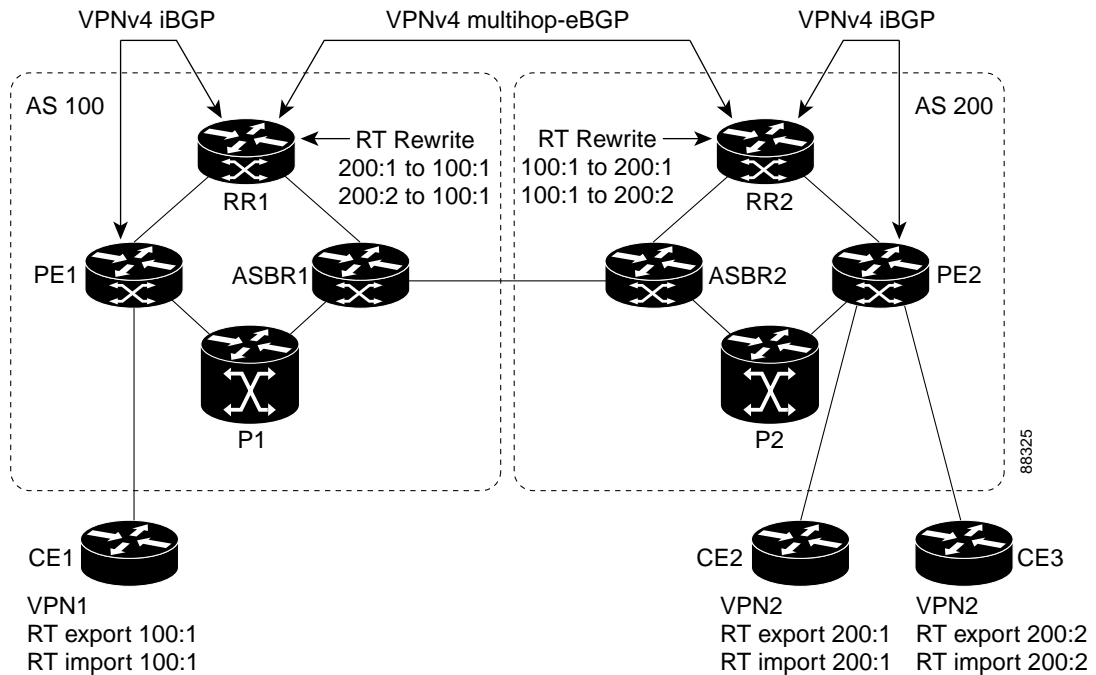


Figure 2 shows an example of route target replacement on route reflectors in an MPLS VPN interautonomous system topology. This example includes the following configurations:

- EBGP is configured on the route reflectors.
- EBGP and IBGP IPv4 label exchange is configured between all BGP routers.
- Peer groups are configured on the routers reflectors.
- PE2 is configured to import and export RT 200:1 for VRF VPN2.
- PE2 is configured to import and export RT 200:2 for VRF VPN3.
- PE1 is configured to import and export RT 100:1 for VRF VPN1.
- RR1 is configured to rewrite all inbound VPNv4 prefixes with RT 200:1 or RT 200:2 to RT 100:1.
- RR2 is configured to rewrite all inbound prefixes with RT 100:1 to RT 200:1 and RT 200:2.

**Figure 2** *Route Target Rewrite on Route Reflectors in an MPLS VPN Interautonomous System Topology*



## Route Maps and Route Target Replacement

The MPLS VPN—Route Target Rewrite feature extends the BGP inbound/outbound route map functionality to enable route target replacement. The **set extcomm-list delete** command entered in route-map configuration mode allows the deletion of a route target extended community attribute based on an extended community list.

## How to Configure MPLS VPN—Route Target Rewrite

This section contains the following procedures to configure MPLS VPN—Route Target Rewrite:

- [Configuring a Route Target Replacement Policy, page 4](#) (required)
- [Applying the Route Target Replacement Policy, page 8](#) (required)
- [Verifying the Route Target Replacement Policy, page 12](#) (optional)
- [Troubleshooting Your Route Target Replacement Policy, page 13](#) (optional)

## Configuring a Route Target Replacement Policy

Perform this task to configure an RT replacement policy for your internetwork.

If you configure a PE to rewrite RT *x* to RT *y* and the PE has a VRF that imports RT *x*, you need to configure the VRF to import RT *y* in addition to RT *x*.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip extcommunity-list** { *standard-list-number* | *expanded-list-number* } { **permit** | **deny** } [*regular-expression*] [**rt** | **soo** *extended-community-value*]
4. **route-map** *map-name* [**permit** | **deny**] [*sequence-number*]
5. **match extcommunity** { *standard-list-number* | *expanded-list-number* }
6. **set extcomm-list** *extended-community-list-number* **delete**
7. **set extcommunity** { **rt** *extended-community-value* [**additive**] | **soo** *extended-community-value* }
8. **end**
9. **show route-map** *map-name*

## DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                          |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                  |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                  |

| Command or Action                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 3</b></p> <pre>ip extcommunity-list {standard-list-number   expanded-list-number} {permit   deny} [regular-expression] [rt   soo extended-community-value]</pre> <p><b>Example:</b></p> <pre>Router(config)# ip extcommunity-list 1 permit rt 100:3</pre> | <p>Creates an extended community access list and controls access to it.</p> <ul style="list-style-type: none"> <li>• The <i>standard-list-number</i> argument is an integer from 1 to 99 that identifies one or more permit or deny groups of extended communities.</li> <li>• The <i>expanded-list-number</i> argument is an integer from 100 to 500 that identifies one or more permit or deny groups of extended communities. Regular expressions can be configured with expanded lists but not standard lists.</li> <li>• The <b>permit</b> keyword permits access for a matching condition.</li> <li>• The <b>deny</b> keyword denies access for a matching condition.</li> <li>• The <i>regular-expression</i> argument specifies an input string pattern to match against. When you use an expanded extended community list to match route targets, include the pattern RT: in the regular expression.</li> <li>• The <b>rt</b> keyword specifies the route target extended community attribute. The <b>rt</b> keyword can be configured only with standard extended community lists and not expanded community lists.</li> <li>• The <b>soo</b> keyword specifies the site of origin (SOO) extended community attribute. The <b>soo</b> keyword can be configured only with standard extended community lists and not expanded community lists.</li> <li>• The <i>extended-community-value</i> argument specifies the route target or site of origin. The value can be one of the following combinations: <ul style="list-style-type: none"> <li>– autonomous-system-number:network-number</li> <li>– ip-address:network-number</li> </ul> <p>The colon is used to separate the autonomous system number and network number or IP address and network number.</p> </li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <p><b>Command:</b></p> <pre>route-map map-name [permit   deny] [sequence-number]</pre> <p><b>Example:</b></p> <pre>Router(config)# route-map extmap permit 10</pre>                                                                                                   | <p>Defines the conditions for redistributing routes from one routing protocol into another or enables policy routing and enables route-map configuration mode.</p> <ul style="list-style-type: none"> <li>The <i>map-name</i> argument defines a meaningful name for the route map. The <b>redistribute</b> router configuration command uses this name to reference this route map. Multiple route maps may share the same map name.</li> <li>If the match criteria are met for this route map, and the <b>permit</b> keyword is specified, the route is redistributed as controlled by the set actions. In the case of policy routing, the packet is policy routed.</li> </ul> <p>If the match criteria are not met, and the <b>permit</b> keyword is specified, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.</p> <p>The <b>permit</b> keyword is the default.</p> <ul style="list-style-type: none"> <li>If the match criteria are met for the route map and the <b>deny</b> keyword is specified, the route is not redistributed. In the case of policy routing, the packet is not policy routed, and no further route maps sharing the same map tag name will be examined. If the packet is not policy routed, the normal forwarding algorithm is used.</li> <li>The <i>sequence-number</i> argument is a number that indicates the position a new route map will have in the list of route maps already configured with the same name. If given with the <b>no</b> form of this command, the position of the route map should be deleted.</li> </ul> |
| Step 5 | <p><b>Command:</b></p> <pre>match extcommunity {standard-list-number  expanded-list-number}</pre> <p><b>Example:</b></p> <pre>Router(config-route-map)# match extcommunity 1</pre> <p><b>Example:</b></p> <pre>Router(config-route-map)# match extcommunity 101</pre> | <p>Matches BGP extended community list attributes.</p> <ul style="list-style-type: none"> <li>The <i>standard-list-number</i> argument is a number from 1 to 99 that identifies one or more permit or deny groups of extended community attributes.</li> <li>The <i>expanded-list-number</i> argument is a number from 100 to 500 that identifies one or more permit or deny groups of extended community attributes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 6 | <p><b>Command:</b></p> <pre>set extcomm-list extended-community-list-number delete</pre> <p><b>Example:</b></p> <pre>Router(config-route-map)# set extcomm-list 1 delete</pre>                                                                                        | <p>Removes a route target from an extended community attribute of an inbound or outbound BGP VPNv4 update.</p> <ul style="list-style-type: none"> <li>The <i>extended-community-list-number</i> argument specifies the extended community list number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|        | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <pre>set extcommunity {rt extended-community-value [additive]   soo extended-community-value}</pre> <p><b>Example:</b><br/>Router(config-route-map)# set extcommunity rt 100:4 additive</p> | <p>Sets BGP extended community attributes.</p> <ul style="list-style-type: none"> <li>The <b>rt</b> keyword specifies the route target extended community attribute.</li> <li>The <b>soo</b> keyword specifies the site of origin extended community attribute.</li> <li>The <i>extended-community-value</i> argument specifies the value to be set. The value can be one of the following combinations: <ul style="list-style-type: none"> <li>autonomous-system-number : network-number</li> <li>ip-address : network-number</li> </ul> <p>The colon is used to separate the autonomous system number and network number or IP address and network number.</p> </li> <li>The <b>additive</b> keyword adds a route target to the existing route target list without replacing any existing route targets.</li> </ul> |
| Step 8 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-route-map)# end</p>                                                                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 9 | <pre>show route-map map-name</pre> <p><b>Example:</b><br/>Router# show route-map extmap</p>                                                                                                 | <p>(Optional) Use this command to verify that the match and set entries are correct.</p> <ul style="list-style-type: none"> <li>The <i>map-name</i> argument is the name of a specific route map.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## Applying the Route Target Replacement Policy

Perform the following tasks to apply the route target replacement policy to your internetwork:

- [Associating Route Maps with Specific BGP Neighbors, page 8](#)
- [Refreshing BGP Session to Apply Route Target Replacement Policy, page 10](#)

## Associating Route Maps with Specific BGP Neighbors

Perform this task to associate route maps with specific BGP neighbors.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family** **vpn**v4 [**unicast**]

6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **extended** | **standard**]
8. **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                               | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul> <p>Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</p> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 172.10.0.2<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                           |
| Step 5 | <b>address-family vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                      | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                                             |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 172.16.0.2<br>activate                     | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                            |



|        | Command or Action                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <pre>neighbor {ip-address   peer-group-name} send-community [both   extended   standard]</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 172.16.0.2<br/>send-community extended</p> | <p>Specifies that a communities attribute should be sent to a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <b>both</b> keyword sends standard and extended community attributes.</li> <li>The <b>extended</b> keyword sends an extended community attribute.</li> <li>The <b>standard</b> keyword sends a standard community attribute.</li> </ul> |
| Step 8 | <pre>neighbor {ip-address   peer-group-name} route-map map-name {in   out}</pre> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 172.16.0.2<br/>route-map extmap in</p>                   | <p>Apply a route map to incoming or outgoing routes</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP or multiprotocol peer group.</li> <li>The <i>map-name</i> argument specifies the name of a route map.</li> <li>The <b>in</b> keyword applies route map to incoming routes.</li> <li>The <b>out</b> keyword applies route map to outgoing routes.</li> </ul>                                           |
| Step 9 | <pre>end</pre> <p><b>Example:</b><br/>Router(config-router-af)# end</p>                                                                                                                             | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Refreshing BGP Session to Apply Route Target Replacement Policy

Perform this task to refresh the BGP session to apply the RT replacement policy.

After you have defined two routers to be BGP neighbors, the routers form a BGP connection and exchange routing information. If you subsequently change a routing policy, you must reset BGP connections for the configuration change to take effect. After configuring the RT replacement policy and applying it to the target routers in your system, you must refresh the BGP session to put the policy into operation.

### SUMMARY STEPS

1. **enable**
2. **clear ip bgp** { \* | *neighbor-address* | *peer-group-name* [soft [in | out]] } [ipv4 { multicast | unicast } | vpnv4 unicast { soft | in | out }]
3. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>clear ip bgp</b> { *   <i>neighbor-address</i>   <i>peer-group-name</i> [ <b>soft</b> [ <b>in</b>   <b>out</b> ]] [ <b>ipv4</b> { <b>multicast</b>   <b>unicast</b> }   <b>vpn4</b> <b>unicast</b> [ <b>soft</b>   <b>in</b>   <b>out</b> ]]<br><br><b>Example:</b><br>Router# clear ip bgp vpn4 unicast 172.16.0.2 in | Resets a BGP connection using BGP soft reconfiguration. <ul style="list-style-type: none"> <li>The <b>*</b> keyword resets all current BGP sessions.</li> <li>The <i>neighbor-address</i> argument resets only the identified BGP neighbor.</li> <li>The <i>peer-group-name</i> argument resets the specified BGP peer group.</li> <li>The <b>ipv4</b> keyword resets the specified IPv4 address family neighbor or peer group. The <b>multicast</b> or <b>unicast</b> keyword must be specified.</li> <li>The <b>vpn4</b> keyword resets the specified VPNv4 address family neighbor or peer group. The <b>unicast</b> keyword must be specified.</li> <li>The <b>soft</b> keyword indicates a soft reset. Does not reset the session. The <b>in</b> or <b>out</b> keywords do not follow the <b>soft</b> keyword when a connection is cleared under the VPNv4 or IPv4 address family because the <b>soft</b> keyword specifies both.</li> <li>The <b>in</b> and <b>out</b> keywords trigger inbound or outbound soft reconfiguration, respectively. If the <b>in</b> or <b>out</b> keyword is not specified, both inbound and outbound soft reset are triggered.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                                                                  | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Troubleshooting Tips

To determine whether a BGP router supports the route refresh capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

You can issue the **debug ip bgp updates** command on the router where you entered the **clear ip bgp** command to verify that the updates are occurring.

**Note**

Issuing the **debug ip bgp updates** command could impair performance if the router sends or receives a large number of BGP updates.

## Verifying the Route Target Replacement Policy

Perform this task to verify the operation of your RT replacement policy.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4 all *network-address***
3. **exit**

### DETAILED STEPS

#### Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

#### Step 2 **show ip bgp vpnv4 all *network-address***

Use this command to verify that all VPNv4 prefixes with a specified RT extended community attribute are replaced with the proper RT extended community attribute at the ASBRs or route reflectors and to verify that the PE routers receive the rewritten RT extended community attributes from the ASBRs or route reflectors. The following examples verify route target replacement on ABSR1 and ABSR2.

Verify route target replacement on ABSR1:

```
Router# show ip bgp vpnv4 all 172.16.17.17

BGP routing table entry for 100:1:172.16.17.17/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  300
    172.16.11.11 (metric 589) from 172.16.11.11 (172.16.11.11)
      Origin incomplete, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:200:1
```

Verify route target replacement on ABSR2:

```
Router# show ip bgp vpnv4 all 172.16.17.17

BGP routing table entry for 100:1:172.16.17.17/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  100 300
    192.168.1.1 from 192.168.1.1 (172.16.13.13)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: RT:100:1
```

The following examples verify route target replacement on PE1 and PE2.

Verify route target on PE1:

```
Router# show ip bgp vpnv4 all 172.16.17.17

BGP routing table entry for 100:1:172.16.17.17/32, version 13
Paths: (1 available, best #1, table vpn1)
  Advertised to update-groups:
```

```

1
300
192.168.2.1 (via vpn1) from 192.168.2.1 (172.16.19.19)
  Origin incomplete, metric 0, localpref 100, valid, external, best
  Extended Community: RT:200:1

```

Verify route target on PE2:

```
Router# show ip bgp vpnv4 all 172.16.17.17
```

```

BGP routing table entry for 100:1:172.16.17.17/32, version 13
Paths: (1 available, best #1, table vpn1)
  Advertised to update-groups:
    3
100 300
  192.168.1.1 (metric 20) from 172.16.16.16 (172.16.16.16)
    Origin incomplete, localpref 100, valid, internal, best
    Extended Community: RT:100:1

```

### Step 3 exit

Use this command to exit to user EXEC mode:

```

Router# exit
Router>

```

## Troubleshooting Your Route Target Replacement Policy

Perform this task to troubleshoot your RT replacement policy.

### SUMMARY STEPS

1. **enable**
2. **debug ip bgp updates**
3. **show ip bgp vpnv4 all *network-address***
4. **exit**

### DETAILED STEPS

#### Step 1 enable

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```

Router> enable
Router#

```

#### Step 2 debug ip bgp updates

Use the following command to verify that BGP updates are occurring on the ASBR. The ASBR in this example has the IP address 172.16.16.16.

```

Router# debug ip bgp updates

BGP(2): no valid path for 100:1:172.16.20.20/32
BGP(2): no valid path for 100:1:10.0.0.0/8
%BGP-5-ADJCHANGE: neighbor 172.16.16.16 Down User reset

```

```

BGP(2): nettable_walker 100:1:172.16.20.20/32 no RIB
BGP(2): nettable_walker 100:1:192.168.3.0/8 no RIB
BGP(2): 172.16.11.11 computing updates, afi 2, neighbor version 13,
table version 15, starting at 0.0.0.0
BGP(2): 172.16.11.11 send unreachable 100:1:172.16.20.20/32
BGP(2): 172.16.11.11 send UPDATE 100:1:172.16.20.20/32 -- unreachable
BGP(2): 172.16.11.11 send UPDATE 100:1:192.168.3.0/8 -- unreachable
BGP(2): 1 updates (average = 58, maximum = 58)
BGP(2): 172.16.11.11 updates replicated for neighbors: 172.16.11.11
BGP(2): 172.16.11.11 update run completed, afi 2, ran for 0ms,
neighbor version 15, start version 15, throttled to 15
BGP: Import walker start version 13, end version 15
BGP: ... start import cfg version = 30
%BGP-5-ADJCHANGE: neighbor 172.16.16.16 Up
BGP(2): 172.16.16.16 computing updates, afi 2, neighbor version 0,
table version 15, starting at 0.0.0.0
BGP(2): 172.16.16.16 send UPDATE (format) 100:1:172.16.0.0/16,
next 172.16.11.11, metric 0, path 300, extended community RT:2:2
RT:7777:22222222 RT:20000:111 RT:65535:999999999
BGP(2): 172.16.16.16 send UPDATE (prepend, chgflags: 0x0)
100:1:172.16.19.19/32, next 172.16.11.11, metric 0, path 300,
extended community RT:2:2 RT:7777:22222222 RT:20000:111
RT:65535:999999999
BGP(2): 172.16.16.16 send UPDATE (format) 100:1:192.168.2.0/8,
next 172.16.11.11, metric 0, path , extended community
RT:2:2 RT:7777:22222222 RT:20000:111 RT:65535:999999999
BGP(2): 2 updates (average = 111, maximum = 121)
BGP(2): 172.16.16.16 updates replicated for neighbors: 172.16.16.16
BGP(2): 172.16.16.16 update run completed, afi 2, ran for 0ms,
neighbor version 15, start version 15, throttled to 15
BGP(2): 172.16.16.16 rcvd UPDATE w/ attr: nexthop 172.16.15.15,
origin ?, path 200, extended community RT:100:1
BGP(2): 172.16.16.16 rcvd 100:1:192.168.3.0/8
BGP(2): 172.16.16.16 rcvd UPDATE w/ attr: nexthop 172.16.15.15,
origin ?, path 200 400, extended community RT:100:1
BGP(2): 172.16.16.16 rcvd 100:1:172.16.0.0/16
BGP(2): 172.16.16.16 rcvd 100:1:172.16.20.20/32
BGP(2): nettable_walker 100:1:172.16.20.20/32 no RIB
BGP(2): nettable_walker 100:1:192.168.3.0/8 no RIB
BGP: Import walker start version 15, end version 17
BGP: ... start import cfg version = 30
BGP(2): 172.16.11.11 computing updates, afi 2,
neighbor version 15, table version 17,
starting at 0.0.0.0
BGP(2): 172.16.11.11 NEXT_HOP part 1 net 100:1:172.16.20.20/32,
next 172.16.15.15
BGP(2): 172.16.11.11 send UPDATE (format) 100:1:172.16.20.20/32,
next 172.16.15.15, metric 0, path 200 400, extended community
RT:1:1 RT:10000:111 RT:33333:888888888
RT:65535:999999999
BGP(2): 172.16.11.11 NEXT_HOP part 1 net 100:1:10.0.0.0/8,
next 172.16.15.15
BGP(2): 172.16.11.11 send UPDATE (format) 100:1:192.168.3.0/8,
next 172.16.15.15, metric 0, path 200, extended community
RT:1:1 RT:10000:111 RT:33333:888888888 RT:65535:999999999
BGP(2): 2 updates (average = 118, maximum = 121)
BGP(2): 172.16.11.11 updates replicated for neighbors: 172.16.11.11
BGP(2): 172.16.11.11 update run completed, afi 2, ran for 0ms,
neighbor version 17, start version 17, throttled to 17

```

You can also reset the BGP connection using the **clear ip bgp \*** command and enter the **debug ip bgp updates** command again to verify that BGP updates are occurring as shown in the output after the **clear ip bgp** command is entered.

**Step 3** `show ip bgp vpnv4 all network-address`

Use this command to verify that RT extended community attributes are replaced correctly. For example:

```
Router# show ip bgp vpnv4 all 172.16.17.17

BGP routing table entry for 100:1:172.16.17.17/32, version 6
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  100 300
    192.168.1.1 from 192.168.1.1 (172.16.13.13)
      Origin incomplete, localpref 100, valid, external, best
      Extended Community: RT:100:1
```

This example shows VPN address information from the BGP table and verifies that RT extended community attributes are replaced correctly.

**Step 4** `exit`

Use this command to exit to user EXEC mode:

```
Router# exit
Router>
```

## Configuration Examples for MPLS VPN—Route Target Rewrite

This section contains the following configuration examples for the MPLS VPN—Route Target Rewrite feature:

- [Configuring Route Target Replacement Policies: Examples, page 15](#)
- [Applying Route Target Replacement Policies: Examples, page 16](#)

### Configuring Route Target Replacement Policies: Examples

This example shows the RT replacement configuration of an ASBR (ASBR1) that exchanges VPNv4 prefixes with another ASBR (ASBR2). The route map extmap is configured to replace RTs on inbound updates. Any incoming update with RT 100:3 is replaced with RT 200:3. Any other prefixes with an RT whose autonomous system number is 100 is rewritten to RT 200:4.

```
!
ip extcommunity-list 1 permit rt 100:3
ip extcommunity-list 101 permit RT:100:*
!
route-map extmap permit 10
match extcommunity 1
set extcomm-list 1 delete
set extcommunity rt 200:3 additive
!
route-map regexp permit 10
match extcommunity 101
set extcomm-list 101 delete
set extcommunity rt 200:4 additive
!
route-map regexp permit 20
```

This example shows the use of the route-map configuration **continue** command when you need to apply more than one replacement rule on an update. In this example, an incoming update with RT 100:3 is replaced with RT 200:3. Without the **continue 20** command, route-map evaluation would stop when a match on sequence 10 is made. With the **continue 20** command, route-map evaluation continues into sequence 20 even if a match occurs in sequence 10. If the incoming update has an RT 100:4, the router replaces it with RT 200:4.

```
!
ip extcommunity-list 1 permit rt 100:3
ip extcommunity-list 2 permit rt 100:4
!
route-map extmap permit 10
match extcommunity 1
set extcomm-list 1 delete
set extcommunity rt 200:3 additive
continue 20
!
route-map extmap permit 20
match extcommunity 2
set extcomm-list 2 delete
set extcommunity rt 200:4 additive
!
route-map extmap permit 30
```

**Note**

The route-map configuration **continue** command is not supported on outbound route maps.

## Applying Route Target Replacement Policies: Examples

This section contains the following examples:

- [Associating Route Maps with Specific BGP Neighbor: Example, page 16](#)
- [Refreshing the BGP Session to Apply the Route Target Replacement Policy: Example, page 17](#)

### Associating Route Maps with Specific BGP Neighbor: Example

This example shows the association of route map extmap with a BGP neighbor. The BGP inbound route map is configured to replace RTs on incoming updates.

```
router bgp 100
.
.
.
neighbor 172.16.0.2 remote-as 100
.
.
.
!
address family vpnv4
neighbor 172.16.0.2 activate
neighbor 172.16.0.2 send-community extended
neighbor 172.16.0.2 route-map extmap in
```

This example shows the association of the same route map with the outbound BGP neighbor. The route map is configured to replace RTs on outgoing updates.

```
router bgp 100
```

```

.
.
.
neighbor 172.16.0.2 remote-as 100
.
.
.
!
address family vpnv4
neighbor 172.16.0.2 activate
neighbor 172.16.0.2 send-community extended
neighbor 172.16.0.2 route-map extmap out

```

## Refreshing the BGP Session to Apply the Route Target Replacement Policy: Example

The following example shows the **clear ip bgp** command used to initiate a dynamic reconfiguration in the BGP peer 172.16.0.2. This command requires that the peer supports the route refresh capability.

```
Router# clear ip bgp 172.16.0.2 vpnv4 unicast in
```

## Additional References

The following sections provide references related to the MPLS VPN—Route Target Rewrite feature.

## Related Documents

| Related Topic                                                            | Document Title                                                              |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| MPLS, MPLS VPN, and MPLS VPN interautonomous systems configuration tasks | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a> |
| Commands to configure MPLS and MPLS VPNs                                 | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>   |
| BGP configuration tasks                                                  | <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a>          |
| Commands to configure and monitor BGP                                    | <a href="#">Cisco IOS IP Routing Protocols Command Reference</a>            |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |



## MIBs

| MIBs                                                                                                                        | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFCs                                                                                                                        | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mps/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mps/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **set extcomm-list delete**

# Feature Information for MPLS VPN—Route Target Rewrite

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—Route Target Rewrite

| Feature Name                  | Releases                                                          | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Route Target Rewrite | 12.0(26)S<br>12.2(25)S<br>12.2(33)SRA<br>12.2(33)SXH<br>12.4(20)T | <p>The MPLS VPN—Route Target Rewrite feature allows the replacement of route targets on incoming and outgoing Border Gateway Protocol (BGP) updates. Typically, Autonomous System Border Routers (ASBRs) perform the replacement of route targets at autonomous system boundaries. Route Reflectors (RRs) and provider edge (PE) routers can also perform route target replacement.</p> <p>The main advantage of the MPLS VPN—Route Target Rewrite feature is that it keeps the administration of routing policy local to the autonomous system.</p> <p>In 12.0(26)S, this feature was introduced for the Cisco 7200, 7500, and 12000 series routers.</p> <p>In 12.2(25)S, this feature was integrated into a Cisco IOS 12.2S release to support the Cisco 7500 series router.</p> <p>In 12.2(33)SRA, this feature was integrated into a Cisco IOS 12.2SRA release.</p> <p>In 12.2(33)SXH, this feature was integrated into a Cisco IOS 12.2SXH release.</p> <p>In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Route Target Replacement Policy, page 2</a></li> <li>• <a href="#">Route Maps and Route Target Replacement, page 4</a></li> <li>• <a href="#">Configuring a Route Target Replacement Policy, page 4</a></li> <li>• <a href="#">Verifying the Route Target Replacement Policy, page 12</a></li> <li>• <a href="#">Troubleshooting Your Route Target Replacement Policy, page 13</a></li> </ul> <p>The following command was modified: <b>set extcomm-list delete</b>.</p> |

# Glossary

**autonomous system**—A collection of networks that share the same routing protocol and that are under the same system administration.

**ASBR**—autonomous system border router. A router that connects and exchanges information between two or more autonomous systems.

**BGP**—Border Gateway Protocol. The exterior border gateway protocol used to exchange routing information between routers in separate autonomous systems. BGP uses Transmission Control Protocol (TCP). Because TCP is a reliable protocol, BGP does not experience problems with dropped or fragmented data packets.

**CE router**—customer edge router. The customer router that connects to the provider edge (PE) router.

**EBGP**—External Border Gateway Protocol. A BGP session between routers in different autonomous systems. When a pair of routers in different autonomous systems are more than one IP hop away from each other, an EBGP session between those two routers is called multihop EBGP.

**IBGP**—Internal Border Gateway Protocol. A BGP session between routers within the same autonomous system.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Internal Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LER**—label edge router. The edge router that performs label imposition and disposition.

**LSR**—label switch router. The role of an LSR is to forward packets in an MPLS network by looking only at the fixed-length label.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**NLRI**—Network Layer Reachability Information. BGP sends routing update messages containing NLRI, which describes the route. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes. The route attributes include a BGP next-hop gateway address, community values, and other information.

**P router**—provider router. The core router in the service provider network that connects to provider edge (PE) routers. In a packet-switched star topology, a router that is part of the backbone and that serves as the single pipe through which all traffic from peripheral networks must pass on its way to other peripheral networks.

**PE router**—provider edge router. The label edge router (LER) in the service provider network that connects to the customer edge (CE) router.

**RD**—route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 (VPNv4) prefix.

**RR**—route reflector. A router that advertises, or reflects, IBGP learned routes to other IBGP peers without requiring a full network mesh.

**RT**—route target. Extended community attribute used to identify the VRF routing table into which a prefix is to be imported.

**VPN**—Virtual Private Network. A group of sites that, as a result of a set of administrative policies, can communicate with each other over a shared backbone.

**VPNv4 prefix**—IPv4 prefix preceded by an 8-byte route distinguisher. The VPN addresses are made unique by adding a route distinguisher to the front of the address.

**VRF**—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

© 2003–2008 Cisco Systems, Inc. All rights reserved.





# MPLS VPN—Per VRF Label

---

**First Published: June 29, 2007**

**Last Updated: December 5, 2008**

The MPLS VPN—Per VRF Label feature (hereafter, in this document, referred to as the Per VRF Label feature or the Per VRF feature) allows you to configure a single Virtual Private Network (VPN) label for all local routes in the entire VPN routing and forwarding (VRF) domain on Cisco 6500 routers. This MPLS VPN—Per VRF Label feature incorporates a single (per VRF) VPN label that for *all* local routes in the VRF table.

You can enable (or disable) the MPLS VPN—Per VRF Label feature in global configuration mode. This feature is available for the Cisco 6500 router only.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS VPN—Per VRF Label](#)” section on page 12.

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

## Contents

This document includes the following topics:

- [Prerequisites for the Per VRF Label Feature, page 2](#)
- [Restrictions for the Per VRF Label Feature, page 2](#)
- [Information About the Per VRF Label Feature, page 2](#)
- [How to Configure the Per VRF Label Feature, page 3](#)
- [Configuration Examples for the Per VRF Label feature, page 5](#)



---

**Americas Headquarters:**

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

- [Additional References, page 10](#)
- [Command Reference, page 11](#)
- [Feature Information for MPLS VPN—Per VRF Label, page 12](#)

## Prerequisites for the Per VRF Label Feature

- If your VRF domain has the external/internal Border Gateway Protocol (EIBGP) multipath feature or the Carrier Supporting Carrier (CSC) feature enabled, disable those features before you configure the Per VRF Label feature.
- Before configuring Multiprotocol Label Switching (MPLS) Layer 3 VPNs, you must have MPLS, Label Distribution Protocol (LDP), and Cisco Express Forwarding (CEF) installed in your network. All routers in the core, including the Provider Edge (PE) routers, must be able to support CEF and MPLS forwarding.

## Restrictions for the Per VRF Label Feature

- Enabling the Per VRF Label feature causes BGP reconvergence, which can result in data loss for traffic coming from the MPLS VPN core.

**Note**

You can minimize network disruption by enabling this feature during a scheduled MPLS maintenance window. Also, if possible, avoid enabling this feature on a live router.

- There is no performance degradation when you configure up to 511 VRFs; however, when you add more than 511 VRFs, your network might experience some minor performance degradation (similar to the normal degradation experienced by any of the directly connected VRF prefixes present in the router).
- Per-prefix MPLS counters for VPN prefixes are lost when you enable the Per VRF Label feature.
- You cannot use this feature with CSC and EIBGP multipath features.

## Information About the Per VRF Label Feature

To configure the MPLS VPN—Per VRF Label feature, you should understand the following concept:

- [MPLS VPN—Per VRF Label Functionality, page 2](#)

## MPLS VPN—Per VRF Label Functionality

The PE stores both local and remote routes and includes a label entry for each route. For distributed platforms, the per-prefix labels consume memory. When there are many VRFs and routes, the amount of memory that the per-prefix labels consume can become an issue.

This new Per VRF Label feature allows the advertisement of a single VPN label for local routes throughout the entire VRF. The router uses a new VPN label for the VRF decoding and IP-based lookup to learn where to forward packets for the PE or customer edge (CE) interfaces.

The following conditions apply when you configure the Per VRF Label feature:

- The VRF uses one label for all local routes.
- When you *enable* the Per VRF Label feature, any existing Per VRF Aggregate label is used. If no Per VRF Aggregate label is present, the software creates a new Per VRF label.
- When you *enable* the Per VRF Label feature, the CE router's learned local routes will experience some data loss.  
  
The CE does not lose data when you disable the Per VRF Label feature because when you disable the feature, the configuration reverts to the default labeling configuration of the Cisco 6500 platform, which uses the Per VRF Aggregate label from the local nonCE-sourced routes.
- When you *disable* the Per VRF Label feature, the configuration reverts to the default configuration of the Cisco 6500 routers.
- A Per VRF label forwarding entry is deleted only if the VRF or the BGP configuration is removed.

#### Summarization of Label Allocation Modes

Table 1 defines the label allocations used with various route types.

**Table 1**      **Label Allocation Modes**

| Route Types                                                                              | Label Mode:<br>Cisco 6500 Default | Label Mode:<br>Per VRF Label Feature |
|------------------------------------------------------------------------------------------|-----------------------------------|--------------------------------------|
| Local to the PE (connected, static route to NULL0, BGP aggregates), redistributed to BGP | Per VRF Aggregate label           | Per VRF label                        |
| Locally learned from CE (through EBGp or other PE or CE protocols)                       | Per Prefix label                  | Per VRF label                        |

## How to Configure the Per VRF Label Feature

This section describes the following required task:

- [Configuring the Per VRF Label Feature, page 3](#)

### Configuring the Per VRF Label Feature

To configure the Per VRF Label feature, perform the following task.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label mode { vrf *vrf-name* | all-vrfs } protocol bgp-vpnv4 { per-prefix | per-vrf }**
4. **end**
5. **show ip vrf detail**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                                        | Purpose                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                           | Enters global configuration mode.                                                                                |
| Step 3 | <b>mpls label mode {vrf vrf-name   all-vrfs} protocol bgp-vpnv4 {per-prefix   per-vrf}</b><br><br><b>Example:</b><br>Router(config)# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf | Configures the Per VRF Label feature.                                                                            |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                 | Returns to privileged EXEC mode.                                                                                 |
| Step 5 | <b>show ip vrf detail</b><br><br><b>Example:</b><br>Router# show ip vrf detail                                                                                                           | Displays the VRF label mode.                                                                                     |

## Examples

The following command example shows how to verify the Per VRF Label configuration:

In this example output, the **bold** text indicates the label modes:

```
Router# show ip vrf detail

VRF vpn1; default RD 1:1; default VPNID <not set>
VRF Table ID = 1
  Interfaces:
    Ethernet0/0          Serial5/0          Loopback1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
CSC is not configured.
VRF label allocation mode: per-vrf (Label 19)
VRF vpn2; default RD 2:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Ethernet2/0          Loopback2
  Connected addresses are not in global routing table
  Export VPN route-target communities
```

```

RT:2:1
Import VPN route-target communities
RT:2:1
No import route-map
No export route-map
CSC is not configured.
VRF label allocation mode: per-vrf (Label 20)
VRF vpn3; default RD 3:1; default VPNID <not set>
VRF Table ID = 3
Interfaces:
  Ethernet3/0          Loopback3
Connected addresses are not in global routing table
Export VPN route-target communities
RT:3:1
Import VPN route-target communities
RT:3:1
No import route-map
No export route-map
CSC is not configured.
VRF label allocation mode: per-vrf (Label 23)

Router# show ip bgp vpnv4 all labels

      Network          Next Hop      In label/Out label
Route Distinguisher: 1:1 (vpn1)
  127.0.0.1/32      192.168.1.1      IPv4 VRF Aggr:19/nolabel
  127.0.0.5/32      127.0.0.4        nolabel/19
  192.168.1.0/24    192.168.1.1      IPv4 VRF Aggr:19/nolabel
                   0.0.0.0          IPv4 VRF Aggr:19/aggregate(vpn1)
  192.168.4.0/24    127.0.0.4        nolabel/20
  172.16.0.0/16     0.0.0.0          IPv4 VRF Aggr:19/aggregate(vpn1)
  172.16.128.0/32  192.168.1.1      IPv4 VRF Aggr:19/nolabel
Route Distinguisher: 2:1 (vpn2)
  127.0.2.2/32     0.0.0.0          IPv4 VRF Aggr:20/aggregate(vpn2)
  127.0.0.6/32     192.168.5.1      IPv4 VRF Aggr:20/nolabel
  192.168.5.0/24    0.0.0.0          IPv4 VRF Aggr:20/aggregate(vpn2)
  172.17.128.0/32  192.168.5.1      IPv4 VRF Aggr:20/nolabel
Route Distinguisher: 3:1 (vpn3)
  127.0.3.2/32     0.0.0.0          IPv4 VRF Aggr:23/aggregate(vpn3)
  127.0.0.8/32     192.168.7.1      IPv4 VRF Aggr:23/nolabel
  192.168.7.0/24    0.0.0.0          IPv4 VRF Aggr:23/aggregate(vpn3)
  172.16.128.0/32  192.168.7.1      IPv4 VRF Aggr:23/nolabel

Router# show mpls forwarding-table

Local  Outgoing  Prefix          Bytes tag  Outgoing   Next Hop
tag    tag or VC  or Tunnel Id    switched  interface
16     Pop tag    192.168.3.0/24  0         Et1/0      192.168.2.3
17     Pop tag    127.0.0.3/32   0         Et1/0      192.168.2.3
18     17        127.0.0.4/32   0         Et1/0      192.168.2.3
19     Pop Label IPv4 VRF[V]    0         aggregate/vpn1
20     Pop Label IPv4 VRF[V]    0         aggregate/vpn2
23     Pop Label IPv4 VRF[V]    0         aggregate/vpn3

PE1#

```

## Configuration Examples for the Per VRF Label feature

This section shows examples for three different configurations:

- [No Label Mode \(Cisco 6500 Router Default\): Example, page 6](#)

- [Mixed Mode \(with Global Per-Prefix\): Example, page 7](#)
- [Mixed Mode \(with Global Per-VRF\): Example, page 9](#)

## No Label Mode (Cisco 6500 Router Default): Example

The following example shows the default label mode configuration (no label mode) for the Cisco 6500 router.

In this example output, the **bold** text indicates the label modes:

```
Router# show ip vrf detail

VRF vpn1; default RD 1:1; default VPNID <not set>
VRF Table ID = 1
  Interfaces:
    Ethernet0/0          Serial5/0          Loopback1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-prefix
  per-vrf-aggr for connected and BGP aggregates (Label 19)
VRF vpn2; default RD 2:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Ethernet2/0          Loopback2
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:1
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-prefix
  per-vrf-aggr for connected and BGP aggregates (Label 20)
VRF vpn3; default RD 3:1; default VPNID <not set>
VRF Table ID = 3
  Interfaces:
    Ethernet3/0          Loopback3
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:3:1
  Import VPN route-target communities
    RT:3:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-prefix
  per-vrf-aggr for connected and BGP aggregates (Label 23)
Router# show ip bgp vpnv4 all labels

      Network          Next Hop          In label/Out label
Route Distinguisher: 1:1 (vpn1)
  127.0.0.1/32         192.168.1.1         27/nolabel
  127.0.0.5/32         127.0.0.4           nolabel/19
  192.168.1.0/24       192.168.1.1         IPv4 VRF Aggr:19/nolabel
```

```

192.168.4.0/24 0.0.0.0 IPv4 VRF Aggr:19/aggregate(vpn1)
127.0.0.4 nolabel/20
172.16.0.0/16 0.0.0.0 IPv4 VRF Aggr:19/aggregate(vpn1)
172.16.128.0/32 192.168.1.1 28/nolabel
Route Distinguisher: 2:1 (vpn2)
127.0.2.2/32 0.0.0.0 IPv4 VRF Aggr:20/aggregate(vpn2)
127.0.0.6/32 192.168.5.1 21/nolabel
192.168.5.0/24 0.0.0.0 IPv4 VRF Aggr:20/aggregate(vpn2)
172.17.128.0/32 192.168.5.1 22/nolabel
Route Distinguisher: 3:1 (vpn3)
127.0.3.2/32 0.0.0.0 IPv4 VRF Aggr:23/aggregate(vpn3)
127.0.0.8/32 192.168.7.1 24/nolabel
192.168.7.0/24 0.0.0.0 IPv4 VRF Aggr:23/aggregate(vpn3)
172.16.128.0/32 192.168.7.1 25/nolabel

```

Router# **show mpls forwarding-table**

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface    | Next Hop    |
|-----------|--------------------|---------------------|--------------------|-----------------------|-------------|
| 16        | Pop tag            | 192.168.3.0/24      | 0                  | Et1/0                 | 192.168.2.3 |
| 17        | Pop tag            | 127.0.0.3/32        | 0                  | Et1/0                 | 192.168.2.3 |
| 18        | 17                 | 127.0.0.4/32        | 0                  | Et1/0                 | 192.168.2.3 |
| 19        | Pop Label          | IPv4 VRF[V]         | <b>0</b>           | <b>aggregate/vpn1</b> |             |
| 20        | Pop Label          | IPv4 VRF[V]         | <b>0</b>           | <b>aggregate/vpn2</b> |             |
| 21        | Untagged           | 127.0.0.6/32[V]     | 0                  | Et2/0                 | 192.168.5.1 |
| 22        | Untagged           | 172.17.128.0/32[V]0 | 0                  | Et2/0                 | 192.168.5.1 |
| 23        | Pop Label          | IPv4 VRF[V]         | <b>0</b>           | <b>aggregate/vpn3</b> |             |
| 24        | Untagged           | 127.0.0.8/32[V]     | 0                  | Et3/0                 | 192.168.7.1 |
| 25        | Untagged           | 172.16.128.0/32[V]0 | 0                  | Et3/0                 | 192.168.7.1 |
| 27        | Untagged           | 127.0.0.1/32[V]     | 0                  | Et0/0                 | 192.168.1.1 |
| 28        | Untagged           | 172.16.128.0/32[V]0 | 0                  | Et0/0                 | 192.168.1.1 |

## Mixed Mode (with Global Per-Prefix): Example

For this example, the following commands set VPN 1 for per-vrf label mode, VPN 2 for per-prefix label mode, and all remaining VPNs for per-prefix (globally).

In this example output, the **bold** text indicates the label modes:

```

Router# mpls label mode vrf vpn1 protocol bgp-vpnv4 per-vrf
Router# mpls label mode vrf vpn2 protocol bgp-vpnv4 per-prefix

```

Use the following show commands to display the label mode settings:

Router# **show ip vrf detail**

```

VRF vpn1; default RD 1:1; default VPNID <not set>
VRF Table ID = 1
  Interfaces:
    Ethernet0/0          Serial5/0          Loopback1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
CSC is not configured.
VRF label allocation mode: per-vrf (Label 26)
VRF vpn2; default RD 2:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:

```

```

Ethernet2/0          Loopback2
Connected addresses are not in global routing table
Export VPN route-target communities
RT:2:1
Import VPN route-target communities
RT:2:1
No import route-map
No export route-map
CSC is not configured.
VRF label allocation mode: per-prefix
per-vrf-aggr for connected and BGP aggregates (Label 27)
VRF vpn3; default RD 3:1; default VPNID <not set>
VRF Table ID = 3
Interfaces:
Ethernet3/0          Loopback3
Connected addresses are not in global routing table
Export VPN route-target communities
RT:3:1
Import VPN route-target communities
RT:3:1
No import route-map
No export route-map
CSC is not configured.
VRF label allocation mode: per-prefix
per-vrf-aggr for connected and BGP aggregates (Label 28)

```

Router# **show ip bgp vpnv4 all label**

| Network                         | Next Hop    | In label/Out label               |
|---------------------------------|-------------|----------------------------------|
| Route Distinguisher: 1:1 (vpn1) |             |                                  |
| 127.0.0.1/32                    | 192.168.1.1 | IPv4 VRF Aggr:26/nolabel         |
| 127.0.0.5/32                    | 127.0.0.4   | nolabel/19                       |
| 192.168.1.0/24                  | 0.0.0.0     | IPv4 VRF Aggr:26/aggregate(vpn1) |
|                                 | 192.168.1.1 | IPv4 VRF Aggr:26/nolabel         |
| 192.168.4.0/24                  | 127.0.0.4   | nolabel/20                       |
| 172.16.0.0/16                   | 0.0.0.0     | IPv4 VRF Aggr:26/aggregate(vpn1) |
| 172.16.128.0/32                 | 192.168.1.1 | IPv4 VRF Aggr:26/nolabel         |
| Route Distinguisher: 2:1 (vpn2) |             |                                  |
| 127.0.2.2/32                    | 0.0.0.0     | IPv4 VRF Aggr:27/aggregate(vpn2) |
| 127.0.0.6/32                    | 192.168.5.1 | 20/nolabel                       |
| 192.168.5.0/24                  | 0.0.0.0     | IPv4 VRF Aggr:27/aggregate(vpn2) |
| 172.17.128.0/32                 | 192.168.5.1 | 21/nolabel                       |
| Route Distinguisher: 3:1 (vpn3) |             |                                  |
| 127.0.3.2/32                    | 0.0.0.0     | IPv4 VRF Aggr:28/aggregate(vpn3) |
| 127.0.0.8/32                    | 192.168.7.1 | 22/nolabel                       |
| 192.168.7.0/24                  | 0.0.0.0     | IPv4 VRF Aggr:28/aggregate(vpn3) |
| 172.16.128.0/32                 | 192.168.7.1 | 23/nolabel                       |

Router# **show mpls forwarding-table**

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 16        | Pop tag            | 192.168.3.0/24      | 0                  | Et1/0              | 192.168.2.3 |
| 17        | Pop tag            | 127.0.0.3/32        | 0                  | Et1/0              | 192.168.2.3 |
| 18        | 17                 | 127.0.0.4/32        | 0                  | Et1/0              | 192.168.2.3 |
| 20        | Untagged           | 127.0.0.6/32[V]     | 0                  | Et2/0              | 192.168.5.1 |
| 21        | Untagged           | 172.17.128.0/32[V]0 | 0                  | Et2/0              | 192.168.5.1 |
| 22        | Untagged           | 127.0.0.8/32[V]     | 0                  | Et3/0              | 192.168.7.1 |
| 23        | Untagged           | 172.16.128.0/32[V]0 | 0                  | Et3/0              | 192.168.7.1 |
| 26        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn1     |             |
| 27        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn1     |             |
| 28        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn1     |             |

## Mixed Mode (with Global Per-VRF): Example

For this example, the following commands set VPN 1 for per-vrf label mode, VPN 2 for per-prefix label mode, and all remaining VPNs for per-vrf (globally).

In this example output, the **bold** text indicates the label modes:

```
Router# mpls label mode vrf vpn1 protocol bgp-vpnv4 per-vrf
Router# mpls label mode vrf vpn2 protocol bgp-vpnv4 per-prefix
Router# mpls label mode all-vrfs protocol bgp-vpnv4 per-vrf

Router# show ip vrf detail

VRF vpn1; default RD 1:1; default VPNID <not set>
VRF Table ID = 1
  Interfaces:
    Ethernet0/0          Serial5/0          Loopback1
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-vrf (Label 26)
VRF vpn2; default RD 2:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Ethernet2/0          Loopback2
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:1
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-prefix
  per-vrf-aggr for connected and BGP aggregates (Label 27)
VRF vpn3; default RD 3:1; default VPNID <not set>
VRF Table ID = 3
  Interfaces:
    Ethernet3/0          Loopback3
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:3:1
  Import VPN route-target communities
    RT:3:1
  No import route-map
  No export route-map
  CSC is not configured.
  VRF label allocation mode: per-vrf (Label 28)

Router# show ip bgp vpnv4 all label

      Network          Next Hop      In label/Out label
Route Distinguisher: 1:1 (vpn1)
  127.0.0.1/32        192.168.1.1    IPv4 VRF Aggr:26/nolabel
  127.0.0.5/32        127.0.0.4      nolabel/19
  192.168.1.0/24      0.0.0.0        IPv4 VRF Aggr:26/aggregate(vpn1)
                   192.168.1.1    IPv4 VRF Aggr:26/nolabel
  192.168.4.0/24      127.0.0.4      nolabel/20
```

```

172.16.0.0/16      0.0.0.0      IPv4 VRF Aggr:26/aggregate(vpn1)
172.16.128.0/32  192.168.1.1  IPv4 VRF Aggr:26/nolabel
Route Distinguisher: 2:1 (vpn2)
127.0.2.2/32      0.0.0.0      IPv4 VRF Aggr:27/aggregate(vpn2)
127.0.0.6/32      192.168.5.1  20/nolabel
192.168.5.0/24     0.0.0.0      IPv4 VRF Aggr:27/aggregate(vpn2)
172.17.128.0/32   192.168.5.1  21/nolabel
Route Distinguisher: 3:1 (vpn3)
127.0.3.2/32      0.0.0.0      IPv4 VRF Aggr:28/aggregate(vpn3)
127.0.0.8/32      192.168.7.1  IPv4 VRF Aggr:28/nolabel
192.168.7.0/24     0.0.0.0      IPv4 VRF Aggr:28/aggregate(vpn3)
172.16.128.0/32   192.168.7.1  IPv4 VRF Aggr:28/nolabel

```

```
Router# show mpls forwarding-table
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 16        | Pop tag            | 192.168.3.0/24      | 0                  | Et1/0              | 192.168.2.3 |
| 17        | Pop tag            | 127.0.0.3/32        | 0                  | Et1/0              | 192.168.2.3 |
| 18        | 17                 | 127.0.0.4/32        | 0                  | Et1/0              | 192.168.2.3 |
| 20        | Untagged           | 127.0.0.6/32[V]     | 0                  | Et2/0              | 192.168.5.1 |
| 21        | Untagged           | 172.17.128.0/32[V]  | 0                  | Et2/0              | 192.168.5.1 |
| 26        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn1     |             |
| 27        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn2     |             |
| 28        | Pop Label          | IPv4 VRF[V]         | 0                  | aggregate/vpn3     |             |

## Additional References

The following sections provide references related to the Per VRF Label feature.

## Related Documents

| Related Topic | Document Title                                                                                                                            |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPNs     | <i>Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4</i><br><a href="#">Part 4: MPLS Virtual Private Networks</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title           |
|----------|-----------------|
| RFC 2547 | <i>BGP/MPLS</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **debug ip bgp vpnv4 unicast**
- **mpls label mode**



# Feature Information for MPLS VPN—Per VRF Label

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN—Per VRF Label

| Feature Name           | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Per VRF Label | 12.2(33)SRD | <p>This feature allows a user to configure a single VPN label for all local routes in the entire VPN routing and forwarding (VRF) domain on Cisco 6500 routers. The feature incorporates a single (per VRF) VPN label for <i>all</i> local routes in the VRF table.</p> <p>You can enable (or disable) the MPLS VPN—Per VRF Label feature in global configuration mode using a new, hidden, command. This feature is available for the Cisco 6500 router only</p> <p>In 12.2(33)SRD, this feature was integrated.</p> |

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2008 Cisco Systems, Inc. All rights reserved.



# MPLS VPN 6VPE per VRF Label

---

**First Published: February 16, 2007**

**Last Updated: December 2, 2008**

The MPLS VPN 6VPE per VRF Label feature allows you to configure a single Virtual Private Network (VPN) label for all local routes in the entire IPv6 VPN routing and forwarding (VRF) domain on Cisco 7600 routers. This MPLS VPN 6VPE per VRF Label feature incorporates a single (per VRF) VPN label for *all* local IPv6 routes in the VRF table.

You can enable (or disable) the MPLS VPN 6VPE per VRF Label feature in global configuration mode. This feature is available for the Cisco 7600 router only.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN 6VPE per VRF Label” section on page 9](#).

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

## Contents

This document includes the following topics:

- [Prerequisites for the MPLS VPN 6VPE per VRF Label feature, page 2](#)
- [Restrictions for the MPLS VPN 6VPE per VRF Label feature, page 2](#)
- [Information About the MPLS VPN 6VPE per VRF Label feature, page 2](#)
- [How to Configure the MPLS VPN 6VPE per VRF Label Feature, page 3](#)
- [Configuration Examples for MPLS VPN 6VPE per VRF Label, page 5](#)
- [Additional References, page 7](#)



---

**Americas Headquarters:**

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

- [Command Reference, page 8](#)
- [Feature Information for MPLS VPN 6VPE per VRF Label, page 9](#)

## Prerequisites for the MPLS VPN 6VPE per VRF Label feature

- If your VRF domain has the external/internal Border Gateway Protocol (EIBGP) multipath feature or the Carrier Supporting Carrier (CSC) feature enabled, disable those features before you configure the MPLS VPN 6VPE per VRF Label feature.
- Before configuring Multiprotocol Label Switching (MPLS) Layer 3 VPNs, you must have MPLS, Label Distribution Protocol (LDP), and Cisco Express Forwarding installed in your network. All routers in the core, including the provider edge (PE) routers, must be able to support Cisco Express Forwarding and MPLS forwarding.
- Before configuring a 6VPE per VRF label, be sure that the IPv6 address family is configured on that VRF.

## Restrictions for the MPLS VPN 6VPE per VRF Label feature

- Enabling the MPLS VPN 6VPE per VRF Label feature causes BGP reconvergence, which can result in data loss for traffic coming from the MPLS VPN core.

**Note**

You can minimize network disruption by enabling this feature during a scheduled MPLS maintenance window. Also, if possible, avoid enabling this feature on a live router.

- Per-prefix MPLS counters for VPN prefixes are lost when you enable the MPLS VPN 6VPE per VRF Label feature.
- You cannot use this feature with CSC and EIBGP multipath features.

## Information About the MPLS VPN 6VPE per VRF Label feature

To configure the MPLS VPN 6VPE per VRF Label feature, you should understand the following concept:

- [MPLS VPN 6VPE per VRF Label Functionality, page 2](#)

## MPLS VPN 6VPE per VRF Label Functionality

The PE router stores both local and remote routes and includes a label entry for each route. For distributed platforms, the multiplicity of per-prefix labels consume memory. When there are many VRFs and routes, the amount of memory that the per-prefix labels consume can cause performance degradation on some platform devices. To avoid this issue, the MPLS VPN 6VPE per VRF Label feature allows the advertisement of a single VPN label for local routes throughout the entire VRF. The router uses a new VPN label for the VRF decoding and IP-based lookup to learn where to forward packets for the PE or customer edge (CE) interfaces.

The following conditions apply when you configure the MPLS VPN 6VPE per VRF Label feature:

- The VRF uses one label for all local routes.
- When you *enable* the MPLS VPN 6VPE per VRF Label feature, any existing per VRF aggregate label is used. If no per VRF aggregate label is present, the software creates a new 6VPE per VRF label.
- When you *enable* the MPLS VPN 6VPE per VRF Label feature, the CE router's learned local routes will experience some data loss.

The CE does not lose data when you disable the MPLS VPN 6VPE per VRF Label feature because the configuration reverts to the default labeling configuration of the Cisco 7600 platform, which uses the Per VRF Aggregate label from the local nonCE-sourced routes.
- When you *disable* the MPLS VPN 6VPE per VRF Label feature, the configuration reverts to the default configuration of the Cisco 7600 routers.
- A 6VPE Per VRF Label forwarding entry is deleted only if the VRF, the IPv6 VRF address family, or the BGP configuration is removed.

See the [Implementing IPv6 VPN over MPLS \(6VPE\)](#) configuration guide for detailed information about IPv6 VPN services and 6VPE.

#### Summarization of Label Allocation Modes

[Table 1](#) defines the label allocations used with various route types.

**Table 1**      **Label Allocation Modes**

| Route Types                                                                              | Label Mode:<br>Cisco 7600 Default | Label Mode:<br>MPLS VPN 6VPE per VRF Label feature |
|------------------------------------------------------------------------------------------|-----------------------------------|----------------------------------------------------|
| Local to the PE (connected, static route to NULL0, BGP aggregates), redistributed to BGP | Per VRF Aggregate label           | 6VPE Per VRF Label                                 |
| Locally learned from CE (through external BGP or other PE or CE protocols)               | Per Prefix label                  | 6VPE Per VRF Label                                 |

## How to Configure the MPLS VPN 6VPE per VRF Label Feature

This section describes the following required task:

- [Configuring the MPLS VPN 6VPE per VRF Label Feature, page 3](#)

### Configuring the MPLS VPN 6VPE per VRF Label Feature

To configure a single (per VRF) VPN label for *all* local IPv6 routes in the VRF table, perform the following task.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **mpls label mode** {vrf *vrf-name* | **all-vrfs**} **protocol** {**bgp-vpnv6** | **all-afs**}  
    {per-prefix | per-vrf}
4. **end**
5. **show vrf detail** *vrf-name*

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                          | Purpose                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                     | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                             | Enters global configuration mode.                                                                                   |
| Step 3 | <b>mpls label mode</b> {vrf <i>vrf-name</i>   <b>all-vrfs</b> } <b>protocol</b> { <b>bgp-vpnv6</b>   <b>all-afs</b> } {per-prefix   per-vrf}<br><br><b>Example:</b><br>Router(config)# mpls label mode all-vrfs protocol bgp-vpnv6 per-vrf | Configures a single (per VRF) VPN label for <i>all</i> local IPv6 routes in the VRF table.                          |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                                   | Returns to privileged EXEC mode.                                                                                    |
| Step 5 | <b>show vrf detail</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router# show vrf detail vpn1                                                                                                                                              | Displays the VRF label mode for the specified VRF.                                                                  |

## Examples

The following example shows how to verify the 6VPE per VRF label configuration.

In this example output, the **bold** text indicates the 6VPE per VRF label mode for VPN1.

```
Router# show vrf detail vpn1
```

```
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    GE4/1                               Lo1
Address family ipv4 (Table ID = 1 (0x1)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1                               RT:2:2
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

```

VRF label allocation mode: per-prefix
  vrf-conn-aggr for connected and BGP aggregates (Label 17)
Address family ipv6 (Table ID = 503316481 (0x1E000001)):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-vrf (Label 18)

Router# show bgp vpnv6 unicast vrf vpn1 label

Network          Next Hop      In label/Out label
Route Distinguisher: 1:1 (vpn1)
2001:DB8:1:2::/96
                  2001:DB8:1:2::1 IPv6 VRF Aggr:18/nolabel
                  ::          IPv6 VRF Aggr:18/nolabel(vpn1)
2001:DB8:4:5::/96
                  ::FFFF:127.0.0.4
                  nolabel/17
2001:DB8:2::1/128
                  ::          IPv6 VRF Aggr:18/nolabel(vpn1)
2001:DB8:4::1/128
                  ::FFFF:127.0.0.4
                  nolabel/18
2001:DB8:CE2::1/128
                  ::FFFF:127.0.0.4
                  nolabel/19
2001:DB8:CE1::1/128
                  2001:DB8:1:2::1 IPv6 VRF Aggr:18/nolabel

Router# show mpls forwarding

Local  Outgoing    Prefix          Bytes Label  Outgoing  Next Hop
Label  Label or VC  or Tunnel Id    Switched     interface
16     Pop Label    127.0.0.4/32    0            AT3/0/0.1  point2point
17     Pop Label    IPv4 VRF[V]     0            aggregate/vpn1
18     Pop Label    IPv6 VRF[V]     0            aggregate/vpn1

```

## Troubleshooting Tips

The `debug ip bgp vpnv6 unicast` command can help troubleshoot the 6VPE per VRF label configuration.

## Configuration Examples for MPLS VPN 6VPE per VRF Label

This section shows the default label mode configuration example (no label mode) for the Cisco 7600 router:

- [6VPE No Label Mode \(Cisco 7600 Router Default\): Example, page 5](#)

## 6VPE No Label Mode (Cisco 7600 Router Default): Example

The following example shows the 6VPE default label mode configuration (no label mode) for the Cisco 7600 router.

In this example output, the **bold** text indicates the default label mode for VPN1.

```
Router# show vrf detail vpn1
```

```
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    GE4/1          Lo1
  Address family ipv4 (Table ID = 1 (0x1)):
    Connected addresses are not in global routing table
    Export VPN route-target communities
      RT:1:1
    Import VPN route-target communities
      RT:1:1          RT:2:2
    No import route-map
    No export route-map
    VRF label distribution protocol: not configured
    VRF label allocation mode: per-prefix
      vrf-conn-aggr for connected and BGP aggregates (Label 17)
  Address family ipv6 (Table ID = 503316481 (0x1E000001)):
    Connected addresses are not in global routing table
    Export VPN route-target communities
      RT:1:1
    Import VPN route-target communities
      RT:1:1
    No import route-map
    No export route-map
    VRF label distribution protocol: not configured
    VRF label allocation mode: per-prefix
      vrf-conn-aggr for connected and BGP aggregates (Label 18)
```

```
Router# show bgp vpnv6 unicast vrf vpn1 label
```

```
Network          Next Hop      In label/Out label
Route Distinguisher: 1:1 (vpn1)
  2001:DB8:1:2::/96
    2001:DB8:1:2::1 IPv6 VRF Aggr:18/nolabel
    ::             IPv6 VRF Aggr:18/nolabel(vpn1)
  2001:DB8:4:5::/96
    ::FFFF:127.0.0.4
    nolabel/17
  2001:DB8:2::1/128
    ::             IPv6 VRF Aggr:18/nolabel(vpn1)
  2001:DB8:4::1/128
    ::FFFF:127.0.0.4
    nolabel/18
  2001:DB8:CE2::1/128
    ::FFFF:127.0.0.4
    nolabel/19
  2001:DB8:CE1::1/128
    2001:DB8:1:2::1 19/nolabel
```

```
Router# show mpls forwarding
```

| Local Label | Outgoing Label or VC | Prefix or Tunnel Id    | Bytes Switched | Label | Outgoing interface    | Next Hop                 |
|-------------|----------------------|------------------------|----------------|-------|-----------------------|--------------------------|
| 16          | Pop Label            | 127.0.0.4/32           | 0              |       | AT3/0/0.1             | point2point              |
| 17          | Pop Label            | IPv4 VRF[V]            | 0              |       | aggregate/vpn1        |                          |
| <b>18</b>   | <b>Pop Label</b>     | <b>IPv6 VRF[V]</b>     | <b>0</b>       |       | <b>aggregate/vpn1</b> |                          |
| 19          | No Label             | 2001:DB8:CE1::1/128[V] | 0              |       | GE4/1                 | FE80::20C:CFFF:FEAD:A00A |

# Additional References

The following sections provide references related to the MPLS VPN 6VPE per VRF Label feature.

## Related Documents

| Related Topic | Document Title                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPNs     | <ul style="list-style-type: none"><li>• <a href="#">Configuring MPLS Virtual Private Networks</a></li><li>• <a href="#">Implementing IPv6 VPN over MPLS (6VPE)</a></li></ul> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title           |
|----------|-----------------|
| RFC 2547 | <i>BGP/MPLS</i> |



## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **debug ip bgp vpnv6 unicast**
- **mpls label mode (6VPE)**

# Feature Information for MPLS VPN 6VPE per VRF Label

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN 6VPE per VRF Label

| Feature Name                | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN 6VPE per VRF Label | 12.2(33)SRD | <p>This feature allows a user to configure a single VPN label for all local routes in the entire IPv6 VPN routing and forwarding (VRF) domain on Cisco 7600 routers. The feature incorporates a single (per VRF) VPN label for <i>all</i> local IPv6 routes in the VRF table.</p> <p>You can enable (or disable) the MPLS VPN 6VPE per VRF Label feature in global configuration mode. This feature is available for the Cisco 7600 only.</p> <p>In Release 12.2(33)SRD, this feature was introduced on the Cisco 7600 router. The following commands were introduced: <b>debug ip bgp vpnv6 unicast</b> and <b>mpls label mode (6VPE)</b>.</p> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLNNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2008 Cisco Systems, Inc. All rights reserved.





# MPLS Multi-VRF (VRF-Lite)

---

**First Published: January 1, 2000**

**Last Updated: July 30, 2008**

The MPLS Multi-VRF feature allows you to configure and maintain more than one instance of a routing and forwarding table within the same customer edge (CE) router.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS Multi-VRF](#)” section on page 18.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS Multi-VRF, page 1](#)
- [Restrictions with MPLS Multi-VRF, page 2](#)
- [Information About MPLS Multi-VRF, page 2](#)
- [How to Configure MPLS Multi-VRF, page 4](#)
- [Configuration Examples for MPLS Multi-VRF, page 13](#)

## Prerequisites for MPLS Multi-VRF

The network’s core and provider edge routers must be configured for MPLS Virtual Private Network (VPN) operation.



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

## Restrictions with MPLS Multi-VRF

You can configure the MPLS Multi-VRF feature only on Layer 3 interfaces.

The MPLS Multi-VRF feature is not supported by Interior Gateway Routing Protocol (IGRP) nor IS-IS.

Label distribution for a given VPN routing and forwarding (VRF) instance on a given router can be handled by either Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP), but not by both protocols at the same time.

Multicast cannot operate on a Layer 3 interface that is configured with the MPLS Multi-VRF feature.

## Information About MPLS Multi-VRF

To configure subscription-based Cisco IOS content filtering, you should understand the following concepts:

- [How the MPLS Multi-VRF Feature Works, page 2](#)
- [How Packets Are Forwarded in a Network Using the MPLS Multi-VRF Feature, page 3](#)

## How the MPLS Multi-VRF Feature Works

The MPLS Multi-VRF feature enables a service provider to support two or more VPNs, where the IP addresses can overlap several VPNs. The MPLS Multi-VRF feature uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN Switched Virtual Interfaces (SVIs), but a Layer 3 interface cannot belong to more than one VRF at any one time. The Multi-VRF feature allows an operator to support two or more routing domains on a CE router, with each routing domain having its own set of interfaces and its own set of routing and forwarding tables. The MPLS Multi-VRF feature makes it possible to extend the Label Switched Paths (LSPs) to the CE and into each routing domain that the CE supports.

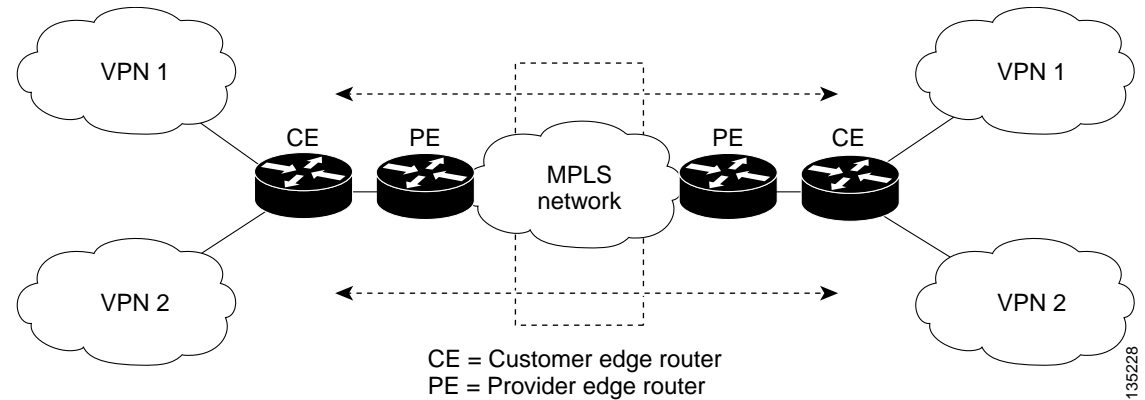
The MPLS Multi-VRF feature works as follows:

- Each CE router advertises its site's local routes to a provider edge (PE) router and learns the remote VPN routes from that PE router.
- PE routers exchange routing information with CE routers by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.
- PE routers exchange MPLS label information with CE routers through LDP or BGP.
- The PE router needs to maintain VPN routes only for those VPNs to which it is directly attached, eliminating the requirement that the PE maintain all of the service provider's VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Two or more interfaces on a PE router can be associated with a single VRF if all the sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CE routers, the PE router exchanges VPN routing information with other PE routers through internal BGP (iBGP).

With the MPLS Multi-VRF feature, two or more customers can share one CE router, and only one physical link is used between the CE and the PE routers. The shared CE router maintains separate VRF tables for each customer and routes packets for each customer based on that customer's own routing table. The MPLS Multi-VRF feature extends limited PE router functionality to a CE router, giving it the ability, through the maintenance of separate VRF tables, to extend the privacy and security of a VPN to the branch office.

Figure 1 shows a configuration where each CE router acts as if it were two CE routers. Because the MPLS Multi-VRF feature is a Layer 3 feature, each interface associated with a VRF must be a Layer 3 interface.

**Figure 1** Each CE Router Acting as Several Virtual CE Routers



## How Packets Are Forwarded in a Network Using the MPLS Multi-VRF Feature

Following is the packet-forwarding process in an MPLS Multi-VRF CE-enabled network, as illustrated in Figure 1:

- When the CE receives a packet from a VPN, it looks up the routing table based on the input interface. When a route is found, the CE imposes the MPLS label it received from the PE for that route and forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it swaps the incoming label with the corresponding label stack and sends it to the MPLS network.
- When an egress PE receives a packet from the network, it swaps the VPN label with the label it earlier had received for the route from the CE, and forwards it to the CE.
- When a CE receives a packet from an egress PE, it uses the incoming label on the packet to forward the packet to the correct VPN.

To configure Multi-VRF, you create a VRF table and then specify the Layer 3 interface associated with that VRF. Next, you configure the routing protocols within the VPN, and between the CE and the PE. BGP is the preferred routing protocol for distributing VPN routing information across the provider's backbone, for reasons that will be detailed in the section, [How to Configure MPLS Multi-VRF, page 4](#).

The Multi-VRF network has three major components:

- **VPN route target communities:** These are lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.
- **Multiprotocol BGP peering of VPN community PE routers:** This propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.
- **VPN forwarding:** This transports all traffic between VPN community members across a VPN service-provider network.

# How to Configure MPLS Multi-VRF

This section contains the following procedures:

- [Configuring VRFs, page 4](#) (Required)
- [Configuring BGP as the Routing Protocol \(Recommended\), page 6](#) (Required)
- [Configuring PE-to-CE MPLS Forwarding and Signalling with BGP \(Recommended\), page 8](#) (Required)
- [Configuring a Routing Protocol Other Than BGP, page 10](#) (Required)
- [Configuring PE-to-CE MPLS Forwarding and Signalling with LDP, page 11](#) (Required)

When BGP is used as the routing protocol, it can also be used for MPLS label exchange between the PE and CE routers. By contrast, if OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

To configure the MPLS Multi-VRF feature, you create a VRF table and then specify the Layer 3 interface associated with that VRF. Then you configure the routing protocols within the VPN and between the CE and the PE routers.

The Multi-VRF network has three major components:

- **VPN route target communities:** These are lists of all other members of a VPN community. You need to configure VPN route targets for each VPN community member.
- **Multiprotocol BGP peering of VPN community PE routers:** This propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.
- **VPN forwarding:** This transports all traffic between VPN community members across a VPN service provider network.

Consider these points when configuring the MPLS Multi-VRF feature in your network:

- A router with the MPLS Multi-VRF feature is shared by several customers, and each customer has its own routing table.
- Because each customer uses a different VRF table, the same IP addresses can be reused. Overlapping IP addresses are allowed in different VPNs.
- The MPLS Multi-VRF feature lets several customers share the same physical link between the PE and the CE routers. Trunk ports with several VLANs separate packets among the customers. Each customer has its own VLAN.
- For the PE router, there is no difference between using the MPLS Multi-VRF feature or using several CE routers. In [Figure 2](#), for example, four virtual Layer 3 interfaces are connected to the MPLS Multi-VRF CE router.
- The MPLS Multi-VRF feature does not affect the packet switching rate.

## Configuring VRFs

Configure VRFs on both the PE and the CE routers.

## Restrictions

Multicast cannot be configured at the same time on the same Layer 3 interface as the MPLS Multi-VRF feature.

## Default VRF Configuration

If a VRF has not been configured, the router has the following default configuration:

- No VRFs have been defined.
- No import maps, export maps, or route maps have been defined.
- No VRF maximum routes exist.
- Only the global routing table exists on the interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip vrf vrf-name**
5. **rd route-distinguisher**
6. **route-target { export | import | both } route-target-ext-community**
7. **import map route-map**
8. **exit**
9. **interface interface-id**
10. **ip vrf forwarding vrf-name**
11. **show ip vrf**

## DETAILED STEPS

|        | Command or Action                                                              | Purpose                                                                                                               |
|--------|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                     |
| Step 3 | <b>ip routing</b><br><br><b>Example:</b><br>Router(config)# ip routing         | Enables IP routing.                                                                                                   |



|         | Command or Action                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                 |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <code>ip vrf vrf-name</code><br><br><b>Example:</b><br>Router(config)# ip vrf v1                                                                                      | Names the VRF, and enters VRF configuration mode.                                                                                                                                                                                                                                                       |
| Step 5  | <code>rd route-distinguisher</code><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1                                                                            | Creates a VRF table by specifying a route distinguisher.<br>Enter either an autonomous system number and an arbitrary number (xxx:y), or an IP address and an arbitrary number (A.B.C.D:y).                                                                                                             |
| Step 6  | <code>route-target {export   import   both}</code><br><code>route-target-ext-community</code><br><br><b>Example:</b><br>Router(config-vrf)# route-target export 100:1 | Creates a list of import, export, or import and export route target communities for the specified VRF.<br>Enter either an autonomous system number and an arbitrary number (xxx:y), or an IP address and an arbitrary number (A.B.C.D:y).<br><br><b>Note</b> This command works only if BGP is running. |
| Step 7  | <code>import map route-map</code><br><br><b>Example:</b><br>Router(config-vrf)# import map importmap1                                                                 | (Optional) Associates a route map with the VRF.                                                                                                                                                                                                                                                         |
| Step 8  | <code>exit</code><br><br><b>Example:</b><br>Router(config-vrf)# exit                                                                                                  | Returns to global configuration mode.                                                                                                                                                                                                                                                                   |
| Step 9  | <code>interface interface-id</code><br><br><b>Example:</b><br>Router(config)# interface fastethernet3/0.10                                                            | Specifies the Layer 3 interface to be associated with the VRF and enters interface configuration mode.<br>The interface can be a routed port or an SVI.                                                                                                                                                 |
| Step 10 | <code>ip vrf forwarding vrf-name</code><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding v1                                                             | Associates the VRF with the Layer 3 interface.                                                                                                                                                                                                                                                          |
| Step 11 | <code>show ip vrf</code><br><br><b>Example:</b><br>Router# show ip vrf                                                                                                | Displays the settings of the VRFs.                                                                                                                                                                                                                                                                      |

## Configuring BGP as the Routing Protocol (Recommended)

Most routing protocols can be used between the CE and the PE routers. However, external BGP (eBGP) is recommended, because:

- BGP does not require more than one algorithm to communicate with many CE routers.
- BGP is designed to pass routing information between systems run by different administrations.
- BGP makes it easy to pass attributes of the routes to the CE router.

When BGP is used as the routing protocol, it can also be used to handle the MPLS label exchange between the PE and CE routers. By contrast, if OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

To configure a BGP PE-to-CE routing session, perform the following steps on the CE and on the PE routers.

## PSUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **network** *ip-address* **mask** *network-mask*
5. **redistribute ospf** *process-id* **match internal**
6. **network** *ip-address* **area** *area-id*
7. **address-family ipv4 vrf** *vrf-name*
8. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
9. **neighbor** *address* **activate**

## DETAILED STEPS

|        | Command                                                                                                                                                           | Purpose                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                     |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                    | Enters global configuration mode.                                                                                                       |
| Step 3 | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                        | Configures the BGP routing process with the autonomous system number passed to other BGP routers, and enters router configuration mode. |
| Step 4 | <b>network</b> <i>ip-address</i> <b>mask</b> <i>network-mask</i><br><br><b>Example:</b><br>Router(config-router)# network<br>10.0.0.0 mask 255.255.255.0          | Specifies a network and mask to announce using BGP.                                                                                     |
| Step 5 | <b>redistribute ospf</b> <i>process-id</i> <b>match</b><br><b>internal</b><br><br><b>Example:</b><br>Router(config-router)# redistribute<br>ospf 2 match internal | Sets the router to redistribute OSPF internal routes.                                                                                   |

|        | Command                                                                                                                                                                                    | Purpose                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>network</b> <i>ip-address</i> <b>area</b> <i>area-id</i><br><br><b>Example:</b><br>Router(config-router)# network<br>10.0.0.0 255.255.255.0 area 0                                      | Identifies the network address and mask on which OSPF is running, and the area ID of that network address.                           |
| Step 7 | <b>address-family</b> <b>ipv4</b> <b>vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-router)# address-family<br>ipv4 vrf v12                                               | Identifies the name of the VRF instance that will be associated with the next two commands, and enters VRF address-family mode.      |
| Step 8 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor<br>10.0.0.3 remote-as 100 | Informs this router's BGP neighbor table of the neighbor's address (or peer group name) and the neighbor's autonomous system number. |
| Step 9 | <b>neighbor</b> <i>address</i> <b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor<br>10.0.0.3 activate                                                           | Activates the advertisement of the IPv4 address-family neighbors.                                                                    |

## Configuring PE-to-CE MPLS Forwarding and Signalling with BGP (Recommended)

If BGP is used for routing between the PE and the CE routers, configure BGP to signal the labels on the VRF interfaces of both the CE and the PE routers. You must enable signalling globally at the router configuration level and for each interface:

- At the router-configuration level, to enable MPLS label signalling via BGP, use the **neighbor send-label** command).
- At the interface level, to enable MPLS forwarding on the interface used for the PE-to-CE eBGP session, use the **mpls bgp forwarding** command.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family** **ipv4** **vrf** *vrf-name*
5. **neighbor** *address* **send-label**
6. **neighbor** *address* **activate**
7. **end**
8. **configure terminal**
9. **interface** *interface-id*

## 10. mpls bgp forwarding

## DETAILED STEPS

|        | Command                                                                                                                        | Purpose                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                 | Enters global configuration mode.                                                                                                                                                                                                              |
| Step 3 | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                     | Configures the BGP routing process with the autonomous system number passed to other BGP routers and enters router configuration mode.                                                                                                         |
| Step 4 | <b>address-family ipv4 vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-router)#<br>address-family ipv4 vrf v12 | Identifies the name of the VRF instance that will be associated with the next two commands and enters address family configuration mode.                                                                                                       |
| Step 5 | <b>neighbor address send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor<br>10.0.0.3 remote-as 100      | Enables the router to use BGP to distribute MPLS labels along with the IPv4 routes to the peer router(s).<br><br>If a BGP session is running when you issue this command, the command does not take effect until the BGP session is restarted. |
| Step 6 | <b>neighbor address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor<br>10.0.0.3 activate             | Activates the advertisement of the IPv4 address-family neighbors.                                                                                                                                                                              |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                             | Returns to privileged EXEC mode.                                                                                                                                                                                                               |
| Step 8 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                 | Enters global configuration mode.                                                                                                                                                                                                              |

|         | Command                                                                                                        | Purpose                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Step 9  | <b>interface</b> <i>interface-id</i><br><br><b>Example:</b><br>Router(config)# interface<br>fastethernet3/0.10 | Enters interface configuration mode for the interface to be used for the BGP session.<br><br>The interface can be a routed port or an SVI. |
| Step 10 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp<br>forwarding                 | Enables MPLS forwarding on the interface.                                                                                                  |

## Configuring a Routing Protocol Other Than BGP

You can use RIP, EIGRP, OSPF or with static routing. This configuration uses OSPF, but the process is the same for other protocols. If OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

If you use OSPF as the routing protocol between the PE and the CE routers, issue the **capability vrf-lite** command in router configuration mode. See [OSPF Support for Multi-VRF in CE Routers](#) for more information.

## Restrictions

If OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

The MPLS Multi-VRF feature is not supported by IGRP nor IS-IS.

Multicast cannot be configured on the same Layer 3 interface as the MPLS Multi-VRF feature is configured.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id* [**vrf** *vrf-name*]
4. **log-adjacency-changes**
5. **redistribute bgp** *autonomous-system-number* **subnets**
6. **network** *ip-address subnet-mask* **area** *area-id*
7. **show ip ospf**

## DETAILED STEPS

|        | Command or Action                                                                                                                         | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                            | Enters global configuration mode.                                                                                |
| Step 3 | <b>router ospf process-id [vrf vpn-name]</b><br><br><b>Example:</b><br>Router(config)# router ospf 100 vrf v1                             | Enables OSPF routing, specifies a VRF table, and enters router configuration mode.                               |
| Step 4 | <b>log-adjacency-changes</b><br><br><b>Example:</b><br>Router(config-router)# log-adjacency-changes                                       | (Optional) Logs changes in the adjacency state.<br><br>This is the default state.                                |
| Step 5 | <b>redistribute bgp autonomous-system-number subnets</b><br><br><b>Example:</b><br>Router(config-router)# redistribute bgp 800 subnets    | Sets the router to redistribute information from the BGP network to the OSPF network.                            |
| Step 6 | <b>network ip-address subnet-mask area area-id</b><br><br><b>Example:</b><br>Router(config-router)# network 10.0.0.0 255.255.255.0 area 0 | Indicates the network address and mask on which OSPF runs, and the area ID of that network address.              |
| Step 7 | <b>show ip ospf</b><br><br><b>Example:</b><br>Router# show ip ospf                                                                        | Displays information about the OSPF routing processes.                                                           |

## Configuring PE-to-CE MPLS Forwarding and Signalling with LDP

If OSPF, EIGRP, RIP, or static routing is used, LDP must be used to signal labels.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **mpls ip**

## DETAILED STEPS

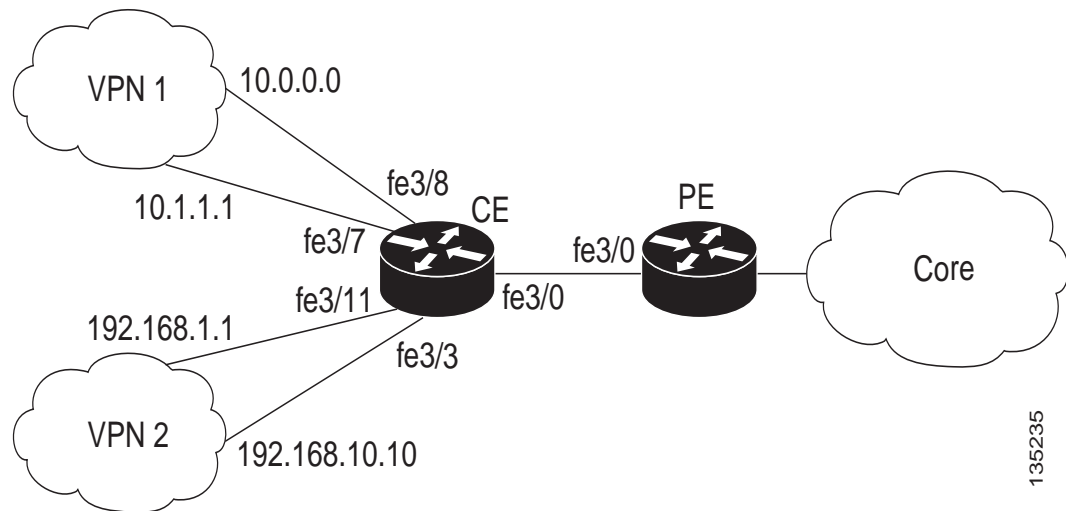
|        | Command or Action                                                            | Purpose                                                                                                                      |
|--------|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code>                                                          | Enables privileged EXEC mode.                                                                                                |
|        | <b>Example:</b><br><code>Router&gt; enable</code>                            | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                           |
| Step 2 | <code>configure terminal</code>                                              | Enters global configuration mode.                                                                                            |
|        | <b>Example:</b><br><code>Router# configure terminal</code>                   |                                                                                                                              |
| Step 3 | <code>interface interface-id</code>                                          | Enters interface configuration mode for the interface associated with the VRF. The interface can be a routed port or an SVI. |
|        | <b>Example:</b><br><code>Router(config)# interface fastethernet3/0.10</code> |                                                                                                                              |
| Step 4 | <code>mpls ip</code>                                                         | Enables MPLS forwarding of IPv4 packets along normally routed paths for this interface.                                      |
|        | <b>Example:</b><br><code>Router(config-if)# mpls ip</code>                   |                                                                                                                              |

# Configuration Examples for MPLS Multi-VRF

This section contains the following examples:

- [Configuring MPLS Multi-VRF on the PE Router: Example, page 13](#)
- [Configuring MPLS Multi-VRF on the CE Router, page 14](#)

**Figure 2** MPLS Multi-VRF Configuration Example



## Configuring MPLS Multi-VRF on the PE Router: Example

### Configuring VRFs

```
configure terminal
ip vrf v1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 exit
ip vrf v2
 rd 100:2
 route-target export 100:2
 route-target import 100:2
 exit
```

### Configuring PE-to-CE connections Using BGP for Both Routing and Label Exchange

```
router bgp 100
 address-family ipv4 vrf v2
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
 exit
 address-family ipv4 vrf v1
  neighbor 10.0.0.8 remote-as 800
  neighbor 10.0.0.8 activate
  neighbor 10.0.0.8 send-label
 end
```



```

configure terminal
interface fastethernet3/0.10
 ip vrf forwarding v1
 ip address 10.0.0.3 255.255.255.0
 mpls bgp forwarding
 exit
interface fastethernet3/0.20
 ip vrf forwarding v2
 ip address 10.0.0.3 255.255.255.0
 mpls bgp forwarding
 exit

```

### Configuring PE-to-CE Connections Using OSPF for Routing and LDP for Label Exchange

```

router ospf 100 vrf v1
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 101 vrf v2
 network 10.0.0.0 255.255.255.0 area 0
 exit
interface fastethernet3/0.10
 ip vrf forwarding v1
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
interface fastethernet3/0.20
 ip vrf forwarding v2
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit

```

## Configuring MPLS Multi-VRF on the CE Router

### Configuring VRFs

```

configure terminal
 ip routing
 ip vrf v11
 rd 800:1
 route-target export 800:1
 route-target import 800:1
 exit
 ip vrf v12
 rd 800:2
 route-target export 800:2
 route-target import 800:2
 exit

```

### Configuring CE Router VPN Connections

```

interface fastethernet3/8
 ip vrf forwarding v11
 ip address 10.0.0.8 255.255.255.0
 exit
interface fastethernet3/11
 ip vrf forwarding v12
 ip address 10.0.0.8 255.255.255.0
 exit
router ospf 1 vrf v11
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit

```

```
router ospf 2 vrf v12
 network 10.0.0.0 255.255.255.0 area 0
 network 10.0.0.0 255.255.255.0 area 0
 exit
```

**Note**

If BGP is used for routing between the PE and CE routers, the BGP-learned routes from the PE router can be redistributed into OSPF using the commands in the following example.

```
router ospf 1 vrf v11
 redistribute bgp 800 subnets
 exit
router ospf 2 vrf v12
 redistribute bgp 800 subnets
 exit
```

**Configuring PE-to-CE Connections Using BGP for Both Routing and Label Exchange**

```
router bgp 800
 address-family ipv4 vrf v12
  neighbor 10.0.0.3 remote-as 100
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 send-label
  redistribute ospf 2 match internal
 exit
 address-family ipv4 vrf v11
  neighbor 10.0.0.3 remote-as 100
  neighbor 10.0.0.3 activate
  neighbor 10.0.0.3 send-label
  redistribute ospf 1 match internal
 end

interface fastethernet3/0.10
 ip vrf forwarding v11
 ip address 10.0.0.8 255.255.255.0
 mpls bgp forwarding
 exit
interface fastethernet3/0.20
 ip vrf forwarding v12
 ip address 10.0.0.8 255.255.255.0
 mpls bgp forwarding
 exit
```

**Configuring PE-to-CE Connections Using OSPF for Routing and LDP for Label Exchange**

```
router ospf 1 vrf v11
 network 10.0.0.0 255.255.255.0 area 0
 exit
router ospf 2 vrf v12
 network 10.0.0.0 255.255.255.0 area 0
 exit

interface fastethernet3/0.10
 ip vrf forwarding v11
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
interface fastethernet3/0.20
 ip vrf forwarding v12
 ip address 10.0.0.3 255.255.255.0
 mpls ip
 exit
```

# Additional References

The following sections provide references related to the MPLS Multi-VRF feature.

## Related Documents

| Related Topic       | Document Title                                                  |
|---------------------|-----------------------------------------------------------------|
| OSPF with Multi-VRF | <i><a href="#">OSPF Support for Multi-VRF in CE Routers</a></i> |

## Standards

| Standard | Title |
|----------|-------|
| N/A      | —     |

## MIBs

| MIB                                                    | MIBs Link                                                                                                                                                                                                                         |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>None</li> </ul> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC | Title |
|-----|-------|
| N/A | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Command Reference

This feature uses no new or modified commands.

# Feature Information for MPLS Multi-VRF

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS Multi-VRF

| Feature Name   | Releases                                                                                       | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS Multi-VRF | 12.1(11)EA1<br>12.1(20)EW<br>12.2(4)T<br>12.2(8)YN<br>12.2(18)SXD<br>12.2(25)EWA<br>12.2(28)SB | The MPLS Multi-VRF feature allows you to configure and maintain more than one instance of a routing and forwarding table within the same CE router.<br><br>In Cisco IOS Release 12.1(11)EA1, the Multi-VRF feature was introduced.<br><br>The feature was integrated into the 12.1(20)EW release.<br><br>The feature was integrated into the 12.2(4)T release.<br><br>The feature was integrated into the 12.2(8)YN release.<br><br>The feature was integrated into the 12.2(18)SXD release.<br><br>The feature was integrated into the 12.2(25)EWA release.<br><br>Multiprotocol Label Switching support was added in Cisco IOS Release 12.2(28)SB. |

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0805R)

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

© 2000-2008 Cisco Systems, Inc. All rights reserved.



# BGP Best External

---

**First Published: November 25, 2009**

**Last Updated: November 25, 2009**

The BGP Best External feature provides the network with a backup external route to avoid loss of connectivity of the primary external route. The BGP Best External feature advertises as a backup route the most preferred route among those received from external neighbors. This feature is beneficial in active-backup topologies, where service providers use routing policies that cause a border router to choose a path received over an internal BGP (iBGP) session (that of another border router) as the best path for a prefix even if it has an external BGP (eBGP) learned path. This active-backup topology defines one exit or egress point for the prefix in the autonomous system and uses the other points as backups if the primary link or eBGP peering is unavailable. The policy causes the border router to hide from the autonomous system the paths that it learned over its eBGP sessions, because it does not advertise any path for such prefixes. To cope with this situation, some routers advertise one externally learned path called the best-external path.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for BGP Best External” section on page 12](#).

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

## Contents

- [Prerequisites for BGP Best External, page 2](#)
- [Restrictions for BGP Best External, page 2](#)
- [Information About BGP Best External, page 2](#)
- [How to Configure BGP Best External, page 5](#)



---

**Americas Headquarters:**

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

- [Configuration Examples for BGP Best External, page 9](#)
- [Additional References, page 10](#)
- [Feature Information for BGP Best External, page 12](#)

## Prerequisites for BGP Best External

- The Bidirectional Forwarding Detection (BFD) protocol must be enabled to quickly detect link failures.
- Ensure that the BGP and the Multiprotocol Label Switching (MPLS) network is up and running with the customer site connected to the provider site by more than one path (multihomed).
- The backup path must have a unique next hop that is not the same as the next hop of the best path.
- BGP must support lossless switchover between operational paths.

## Restrictions for BGP Best External

- The BGP Best External feature will not install a backup path if BGP Multipath is installed and a multipath exists in the BGP table. One of the multipaths automatically acts as a backup for the other paths.
- The BGP Best External feature is not supported with the following features:
  - MPLS VPN Carrier Supporting Carrier
  - MPLS VPN Inter-Autonomous Systems, option B
  - MPLS VPN Per VRF Label
- The BGP Best External feature cannot be configured with Multicast, L2VPNs, or IPv6 VPNs.
- The BGP Best External feature cannot be configured on route reflectors.
- The BGP Best External feature does not support NSF/SSO. However, ISSU is supported if both route processors have the BGP Best External feature configured.
- The BGP Best External feature can only be configured on VPNv4 and IPv4 VRF address families.
- When you configure the BGP Best External feature using the **bgp advertise-best-external** command, you do not need to also enable the BGP PIC feature with the **bgp additional-paths install** command. The BGP PIC feature is automatically enabled by the BGP Best External feature.
- When you configure the BGP Best External feature, it will override the functionality of the [MPLS VPN—BGP Local Convergence](#) feature. However, you do not have to remove the **protection local-prefixes** command from the configuration.

## Information About BGP Best External

Before configuring the BGP Best External feature, you should understand the following concepts:

- [BGP Best External Overview, page 3](#)
- [What the Best External Route Means, page 3](#)
- [How the BGP Best External Feature Works, page 3](#)

- [Configuration Modes for Enabling BGP Best External, page 4](#)

## BGP Best External Overview

Service providers use routing policies that cause a border router to choose a path received over an internal BGP (iBGP) session (that of another border router) as the best path for a prefix even if it has an external BGP (eBGP) learned path. This practice is known popularly as active-backup topology and is done to define one exit or egress point for the prefix in the autonomous system and to use the other points as backups if the primary link or eBGP peering is unavailable.

The policy, though beneficial, causes the border router to hide from the autonomous system the paths that it learned over its eBGP sessions, because it does not advertise any path for such prefixes. To cope with this situation, some routers advertise one externally learned path called the best-external path. The best-external behavior causes the BGP selection process to select two paths to every destination:

- The best path is selected from the complete set of routes known to that destination.
- The best external path is selected from the set of routes received from its external peers.

BGP advertises to external peers the best path. Instead of withdrawing the best path from its internal peers when it selects an iBGP path as the best path, BGP advertises the best external path to the internal peers.

The BGP Best External feature is an essential component of the prefix independent (PIC) edge for both Internet access and MPLS VPN scenarios makes alternate paths available in the network in the active-backup topology.

## What the Best External Route Means

The BGP Best External feature uses a “best external route” as a backup path, which, according to *draft-marques-idr-best-external*, is the most preferred route among those received from external neighbors. The most preferred route from external neighbors can be the following:

- Two routers in different clusters that have an iBGP session between them.
- Two routers in different autonomous systems of a confederation that have an eBGP session between them.

The best external route might be different from the best route installed in the RIB. The best route could be an internal route. By allowing the best external route to be advertised and stored in addition to the best route, networks gain faster restoration of connectivity by providing additional paths that may be used if the primary path fails.

## How the BGP Best External Feature Works

The BGP Best External feature is based on Internet Engineering Task Force (IETF) *draft-marques-idr-best-external.txt*. The BGP Best External feature advertises a best external route to its internal peers as a backup route. The backup route is stored in the routing information base (RIB) and Cisco Express Forwarding. If the primary path fails, the BGP PIC functionality enables the best external path to take over, enabling faster restoration of connectivity.



**Figure 1** *MPLS VPN: Best External at the Edge of MPLS VPN*

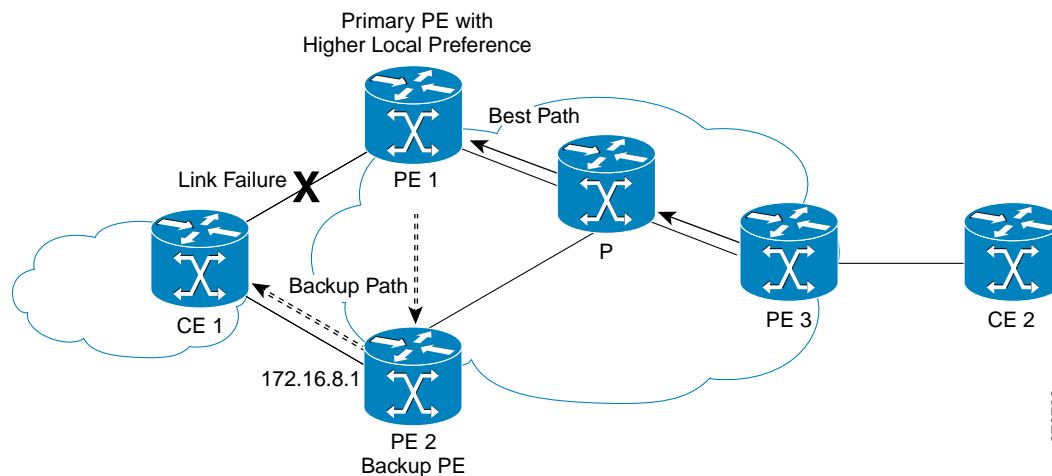


Figure 1 shows an MPLS VPN using the BGP Best External feature. The network includes the following components:

- eBGP sessions exist between the provider edge (PE) and customer edge (CE) routers.
- PE1 is the primary router and has a higher local preference setting.
- Traffic from CE2 uses PE1 to reach router CE1.
- PE1 has two paths to reach CE1.
- CE1 is dual-homed with PE1 and PE2.
- PE1 is the primary path and PE2 is the backup path.

In Figure 1, traffic in the MPLS cloud flows through PE1 to reach CE1. Therefore, PE2 uses PE1 as the best path and PE2 as the backup path.

PE1 and PE2 are configured with the BGP Best External feature. BGP computes both the best path (the PE1–CE1 link) and an backup path (PE2) and installs both paths into the RIB and Cisco Express Forwarding. The best external path (PE2) is advertised to the peer routers in addition to the best path.

When Cisco Express Forwarding detects a link failure on PE1–CE1 link, Cisco Express Forwarding immediately switches to the backup path PE2. Traffic is quickly re-routed very due to local Fast Convergence in Cisco Express Forwarding using the backup path. Thus traffic loss is minimized and fast convergence achieved.

## Configuration Modes for Enabling BGP Best External

You can enable the BGP Best External feature in different modes, each of which protects VRFs in its own way:

- If you issue the **bgp advertise-best-external** command in VPNv4 address family configuration mode, it applies to all IPv4 VRFs. If you issue the command in this mode, you need not also issue it for specific VRFs.
- If you issue the **bgp advertise-best-external** command in IPv4 address-family configuration mode, it applies only that VRF.

# How to Configure BGP Best External

Perform the following tasks to enable the BGP Best External feature.

- [Enabling the BGP Best External Feature, page 5](#)
- [Verifying the BGP Best External Feature, page 7](#)

## Enabling the BGP Best External Feature

Perform the following task to enable the BGP Best External feature. In this task the configuration shown allows the BGP Best External feature to be configured in either IPv4 or VPNv4 address family. In VPNv4 address family configuration mode, the BGP Best External feature applies to all IPv4 VRFs and you do not have to configure it for specific VRFs as well. If you issue the **bgp advertise-best-external** command in IPv4 VRF address family configuration mode, the BGP Best External feature applies only that VRF.

### Prerequisites

- Configure the MPLS VPN and verify that it is working properly before configuring the BGP Best External feature. See [Configuring MPLS Layer 3 VPNs](#) for more information.
- Configure multiprotocol VRFs, which allows you to share route targets policies (import and export) between IPv4 and IPv6 or to configure separate route-target policies for IPv4 and IPv6 VPNs. For information on configuring multiprotocol VRFs, see [MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs](#).
- Ensure that the CE router is connected to the network by at least two paths.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **vrf** *vrf-name*]  
or  
**address-family vpnv4** [**unicast**]
5. **bgp advertise-best-external**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **activate**
8. **neighbor** *ip-address* **fall-over** [**bfd** | **route-map** *map-name*]
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 40000                                                                                                                                                         | Enters router configuration mode for the specified routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <b>address-family ipv4</b> [ <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br>or<br><b>address-family vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 unicast<br>or<br>Router(config-router)# address-family vpnv4 | Specifies the IPv4 or VPNv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 or VPNv4 unicast address family.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                   |
| Step 5 | <b>bgp advertise-best-external</b><br><br><b>Example:</b><br>Router(config-router-af)# bgp advertise-best-external                                                                                                                                                   | Calculates and uses an external backup path and installs it into the RIB and Cisco Express Forwarding.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 6 | <b>neighbor ip-address remote-as</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 remote-as 45000                                                                                                        | Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>By default, neighbors that are defined using the <b>neighbor remote-as</b> command in router configuration mode exchange only IPv4 unicast address prefixes. To exchange other address prefix types, neighbors must also be activated using the <b>neighbor activate</b> command in address family configuration mode for the other prefix types.</li> </ul> |
| Step 7 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 activate                                                                                                                                                | Enables the neighbor to exchange prefixes for the IPv4 unicast address family with the local router.                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|        | Command or Action                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8 | <b>neighbor</b> <i>ip-address</i> <b>fall-over</b> [ <b>bfd</b>   <b>route-map</b> <i>map-name</i> ]<br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 fall-over bfd | Configures the BGP peering to use fast session deactivation and enables BFD protocol support for failover. <ul style="list-style-type: none"> <li>BGP will remove all routes learned through this peer if the session is deactivated.</li> </ul> |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                                          | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                        |

## Verifying the BGP Best External Feature

Perform the following task to verify that the BGP Best External feature is configured correctly.

### SUMMARY STEPS

- enable**
- show vrf detail**
- show ip bgp ipv4 {mdt {all | rd | vrf} | multicast | tunnel | unicast}**  
or  
**show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [rib-failure] [ip-prefix/length [longer-prefixes]] [network-address [mask] [longer-prefixes]] [cidr-only] [community [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]**
- show bgp vpnv4 unicast vrf vrf-name ip-address**
- show ip route vrf vrf-name repair-paths ip-address**
- show ip cef vrf vrf-name ip-address detail**

### DETAILED STEPS

#### Step 1 enable

Use this command to enable privileged EXEC mode. Enter your password, if prompted. For example:

```
Router> enable
Router#
```

#### Step 2 show vrf detail

Use this command to verify that the BGP Best External feature is enabled. The following **show vrf detail** command output shows that the BGP Best External feature is enabled. (Relevant output is shown in bold).

```
Router# show vrf detail

VRF test1 (VRF Id = 1); default RD 400:1; default VPNID <not set>
  Interfaces:
    Se4/0
  Address family ipv4 (Table ID = 1 (0x1)):
    BGP Best External: enabled
```

```

Export VPN route-target communities
  RT:100:1          RT:200:1          RT:300:1
  RT:400:1
Import VPN route-target communities
  RT:100:1          RT:200:1          RT:300:1
  RT:400:1
No import route-map
No export route-map
VRF label distribution protocol: not configured
VRF label allocation mode: per-prefix
Prefix protection with additional path enabled
Address family ipv6 not active.

```

### Step 3 **show ip bgp ipv4 { mdt { all | rd | vrf } | multicast | tunnel | unicast }**

or

**show ip bgp vpnv4 { all | rd route-distinguisher | vrf vrf-name } [rib-failure] [ip-prefix/length [longer-prefixes]] [network-address [mask] [longer-prefixes]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]**

Use this command to verify that the best external route is advertised. In the command output, the code b indicates a backup path and the code x designates the best external path. In the following example, the relevant output is shown in bold.

```
Router# show ip bgp vpnv4 all
```

```

BGP table version is 1104964, local router ID is 10.2.2.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

```

| Network                                           | Next Hop        | Metric   | LocPrf | Weight       | Path |
|---------------------------------------------------|-----------------|----------|--------|--------------|------|
| Route Distinguisher: 11:12 (default for vrf blue) |                 |          |        |              |      |
| *>i1.0.0.1/32                                     | 10.10.3.3       | 0        | 200    | 0 1 ?        |      |
| * i                                               | 10.10.3.3       | 0        | 200    | 0 1 ?        |      |
| *                                                 | 10.0.0.1        |          |        | 0 1 ?        |      |
| <b>*bx</b>                                        | <b>10.0.0.1</b> | <b>0</b> |        | <b>0 1 ?</b> |      |
| *                                                 | 10.0.0.1        |          |        | 0 1 ?        |      |

### Step 4 **show bgp vpnv4 unicast vrf vrf-name ip-address**

Use this command to verify that the best external route is advertised. In the following example, the relevant output is shown in bold.

```
Router# show bgp vpnv4 unicast vrf vpn1 10.10.10.10
```

```

BGP routing table entry for 10:10:10.10.10.10/32, version 10
Paths: (2 available, best #1, table vpn1)
  Advertise-best-external
    Advertised to update-groups:
      1          2
    200
      10.6.6.6 (metric 21) from 10.6.6.6 (10.6.6.6)
      Origin incomplete, metric 0, localpref 200, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out 23/23
    200
      10.1.2.1 from 10.1.2.1 (10.1.1.1)
      Origin incomplete, metric 0, localpref 100, valid, external, backup/repair,
      advertise-best-external
      Extended Community: RT:1:1 , recursive-via-connected
      mpls labels in/out 23/nolabel

```

**Step 5** `show ip route vrf vrf-name repair-paths ip-address`

Use this command to display the repair route, which is shown in bold.

```
Router# show ip route vrf vpn1 repair-paths
```

```
Routing Table: vpn1
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP
        + - replicated route, % - next hop override
```

```
Gateway of last resort is not set
```

```

      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       10.1.1.0/24 [200/0] via 10.6.6.6, 00:38:33
          [RPR][200/0] via 10.1.2.1, 00:38:33
B       10.1.1.1/32 [200/0] via 10.6.6.6, 00:38:33
          [RPR][200/0] via 10.1.2.1, 00:38:33
      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.2.0/24 is directly connected, Ethernet0/0
L       10.1.2.2/32 is directly connected, Ethernet0/0
B       10.1.6.0/24 [200/0] via 10.6.6.6, 00:38:33
          [RPR][200/0] via 10.1.2.1, 00:38:33
```

**Step 6** `show ip cef vrf vrf-name ip-address detail`

Use this command to display the best external route. In the following example, the relevant output is shown in bold.

```
Router# show ip cef vrf test 10.71.8.164 detail
```

```
10.71.8.164/30, epoch 0, flags rib defined all labels
recursive via 10.249.0.102 label 35
  nexthop 10.249.246.101 Ethernet0/0 label 25
recursive via 10.249.0.104 label 28, repair
  nexthop 10.249.246.101 Ethernet0/0 label 24
```

## Configuration Examples for BGP Best External

The following examples configure and then verify the BGP Best External feature:

- [Configuring the BGP Best External Feature: Example, page 9](#)

### Configuring the BGP Best External Feature: Example

The following example configures the BGP Best External feature in VPNv4 mode:

```
vrf definition test1
rd 400:1
route-target export 100:1
route-target export 200:1
route-target export 300:1
route-target export 400:1
route-target import 100:1
route-target import 200:1
```

```

route-target import 300:1
route-target import 400:1
address-family ipv4
exit-address-family
exit
!
interface Ethernet1/0
vrf forwarding test1
ip address 10.0.0.1 255.0.0.0
exit
!
router bgp 64500
no synchronization
bgp log-neighbor-changes
neighbor 10.5.5.5 remote-as 64500
neighbor 10.5.5.5 update-source Loopback0
neighbor 10.6.6.6 remote-as 64500
neighbor 10.6.6.6 update-source Loopback0
no auto-summary
!
address-family vpnv4
bgp advertise-best-external
neighbor 10.5.5.5 activate
neighbor 10.5.5.5 send-community extended
neighbor 10.6.6.6 activate
neighbor 10.6.6.6 send-community extended
exit-address-family
!
address-family ipv4 vrf test1
no synchronization
bgp recursion host
neighbor 192.168.13.2 remote-as 64511
neighbor 192.168.13.2 fall-over bfd
neighbor 192.168.13.2 activate
neighbor 192.168.13.2 as-override
exit-address-family

```

# Additional References

The following sections provide references related to the BGP Best External feature.

## Related Documents

| Related Topic                                                           | Document Title                                          |
|-------------------------------------------------------------------------|---------------------------------------------------------|
| Basic MPLS VPNs                                                         | <a href="#">Configuring MPLS Layer 3 VPNs</a>           |
| Multiprotocol VRFs                                                      | <a href="#">MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs</a> |
| A failover feature that creates a new path after a link or node failure | <a href="#">MPLS VPN—BGP Local Convergence</a>          |
| BGP routing                                                             | <a href="#">BGP Feature Roadmap</a>                     |

## Standards

| Standard                        | Title                                                               |
|---------------------------------|---------------------------------------------------------------------|
| draft-marques-idr-best-external | BGP Best-external, Advertisement of the best-external route to iBGP |

## MIBs

| MIB | MIBs Link                                                                                                                                                                                                              |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N/A | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                      |
|----------|--------------------------------------------|
| RFC 2547 | <i>BGP/MPLS VPNs</i>                       |
| RFC 1771 | <i>A Border Gateway Protocol 4 (BGP-4)</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |



# Feature Information for BGP Best External

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for BGP Best External

| Feature Name      | Releases                   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP Best External | 12.2(33)SRE<br>12.2(33)XNE | <p>The BGP Best External feature creates and stores a backup path in the routing information base and in Cisco Express Forwarding, so that in case of a failure, the backup path can immediately take over, thus enabling subsecond failover.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was introduced.</p> <p>In 12.2(33)XNE, support was added for the Cisco 10000 router.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Information About BGP Best External, page 2</a></li> <li>• <a href="#">How to Configure BGP Best External, page 5</a></li> <li>• <a href="#">Configuration Examples for BGP Best External, page 9</a></li> </ul> <p>The following commands were introduced or modified: <b>bgp advertise-best-external</b>, <b>bgp recursion host</b>, <b>show ip bgp</b>, <b>show ip bgp vpnv4</b>, <b>show ip cef</b>, <b>show ip cef vrf</b>, <b>show ip route</b>, <b>show ip route vrf</b>.</p> |

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.



# BGP PIC Edge for IP and MPLS-VPN

---

**First Published: November 20, 2009**

**Last Updated: November 25, 2009**

The BGP PIC Edge for IP and MPLS-VPN feature improves convergence after a network failure. This convergence is applicable to both core and edge failures and can be used in both IP and MPLS networks. BGP PIC Edge for IP and MPLS-VPN feature creates and stores a backup/alternate path in the routing information base (RIB), forwarding information base (FIB) and in Cisco Express Forwarding, so that when a failure is detected, the backup/alternate path can immediately take over, thus enabling fast failover.

Benefits of this feature include the following:

- An additional path for failover allows faster restoration of connectivity if a primary path is invalid or is withdrawn.
- Reduction of traffic loss.
- Constant convergence time so that the switching time is the same for all prefixes.



**Note**

---

In this document, the BGP PIC Edge for IP and MPLS-VPN feature is called “BGP PIC.”

---

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for BGP PIC” section on page 18](#).

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for BGP PIC, page 2](#)
- [Restrictions for BGP PIC, page 2](#)
- [Information About BGP PIC, page 3](#)
- [How to Configure BGP PIC, page 11](#)
- [Configuration Examples for BGP PIC, page 13](#)
- [Additional References, page 17](#)
- [Feature Information for BGP PIC, page 18](#)

## Prerequisites for BGP PIC

- Ensure that the BGP and the IP or Multiprotocol Label Switching (MPLS) network is up and running with the customer site connected to the provider site by more than one path (multihomed).
- Ensure that the backup/alternate path has a unique next hop that is not the same as the nexthop of the best path.
- Enable Bidirectional Forwarding Detection (BFD) protocol to quickly detect link failures of directly connected neighbors.

## Restrictions for BGP PIC

The following restrictions apply to the BGP PIC feature:

- With BGP Multipath, the BGP PIC feature is already supported.
- In MPLS VPNs, the BGP PIC feature is not supported with MPLS VPN Inter-Autonomous Systems Option B.
- The BGP PIC feature supports prefixes only the IPv4 and VPNv4 address families.
- The BGP PIC feature cannot be configured with Multicast, L2VPNs, or IPv6 VPNs.
- If the route reflector is only in the control plane, then you do not need BGP PIC, because BGP PIC addresses data plane convergence.
- When two PE routers become each other's backup/alternate path to a CE router, traffic might loop if the CE router fails. Neither router will reach the CE router, and traffic will continue to be forwarded between the PE router until the time-to-live (TTL) timer expires.
- The BGP PIC feature does not support NSF/SSO. However, ISSU is supported if both route processors have the BGP PIC feature configured.
- The BGP PIC feature solves the traffic forwarding only for a single network failure at both edge and core.
- The BGP PIC feature does not work with the he BGP Best External feature. If you try to configure the BGP PIC feature after configuring the BGP Best External feature, you receive an error.

# Information About BGP PIC

Before configuring the BGP PIC feature, you should understand the following concepts:

- [How BGP Converges Under Normal Circumstances, page 3](#)
- [How BGP PIC Improves Convergence, page 3](#)
- [How a Failure Is Detected, page 5](#)
- [How BGP PIC Can Achieve Subsecond Convergence, page 5](#)
- [How BGP PIC Improves Upon the Functionality of MPLS VPN—BGP Local Convergence, page 6](#)
- [Configuration Modes for Enabling BGP PIC, page 6](#)
- [BGP PIC Scenarios, page 6](#)

## How BGP Converges Under Normal Circumstances

Under normal circumstances, BGP can take several seconds to a few minutes to converge after a network change. At a high level, BGP goes through the following process:

1. BGP learns of failures through either IGP or BFD events or interface events.
2. BGP withdraws the routes from the routing information base (RIB), and the RIB withdraws the routes from the forwarding information base (FIB) and distributed FIB (dFIB). This process clears the data path for the affected prefixes.
3. BGP sends withdraw messages to its neighbors.
4. BGP calculates the next best path to the affected prefixes.
5. BGP inserts the next best path for affected prefixes into the RIB, and the RIB installs them in the FIB and dFIB.

This process takes from a few seconds to a few minutes to complete depending on the latency of the network, the convergence time across the network, and the local load on the devices. The data plane converges only after the control plane converges.

## How BGP PIC Improves Convergence

BGP PIC functionality is achieved by additional functionality in the BGP, RIB, Cisco Express Forwarding, and MPLS.

- BGP Functionality

BGP PIC affects prefixes under the IPv4 and VPNv4 address families. For those prefixes, BGP calculates an additional second best path in addition to the primary best path. (The second best path is called the backup/alternate path.) BGP installs the best and backup/alternate paths for the affected prefixes into the BGP RIB. The backup/alternate path provides a fast reroute mechanism to counter a singular network failure. BGP also includes the alternate/backup path in its application programming interface (API) to the IP RIB.

- RIB Functionality

For BGP PIC, RIB installs an alternate path per route if one is available. With BGP PIC functionality, if the RIB selects a BGP route containing a backup/alternate path, it installs the backup/alternate path with the best path. The RIB also includes the alternate path in its API with the FIB.

- Cisco Express Forwarding (FIB) Functionality

With BGP PIC, Cisco Express Forwarding stores an alternate path per prefix. When the primary path goes down, Cisco Express Forwarding searches for the backup/alternate path when in a prefix independent manner. Cisco Express Forwarding also listens to BFD events to rapidly detect local failures.

- MPLS Functionality

MPLS Forwarding is similar to Cisco Express Forwarding in that it stores alternate paths and switches to an the alternate path if the primary path goes away.

When the BGP PIC feature is enabled, BGP calculates a backup/alternate path per prefix and installs them into BGP RIB, IP RIB, and FIB. This improves convergence after a network failure. There are two types of network failures that the BGP PIC feature detects:

- Core node/link failure (iBGP node failure): If a PE node/link fails, then the failure is detected through IGP convergence. IGP conveys the failure through the RIB to the FIB.
- Local link/immediate neighbor node failure (eBGP node/link failure): To detect a local link failure or eBGP single-hop peer node failure in less than a second, you must enable BFD. Cisco Express Forwarding looks for BFD events to detect a failure of an eBGP single-hop peer.

#### Convergence in the Data Plane

Upon detection of a failure, Cisco Express Forwarding detects the alternate nexthop for all prefixes affected by the failure. The data plane convergence is achieved in subseconds depending on whether the BGP PIC implementation exists software or hardware.

#### Convergence in the Control Plane Convergence

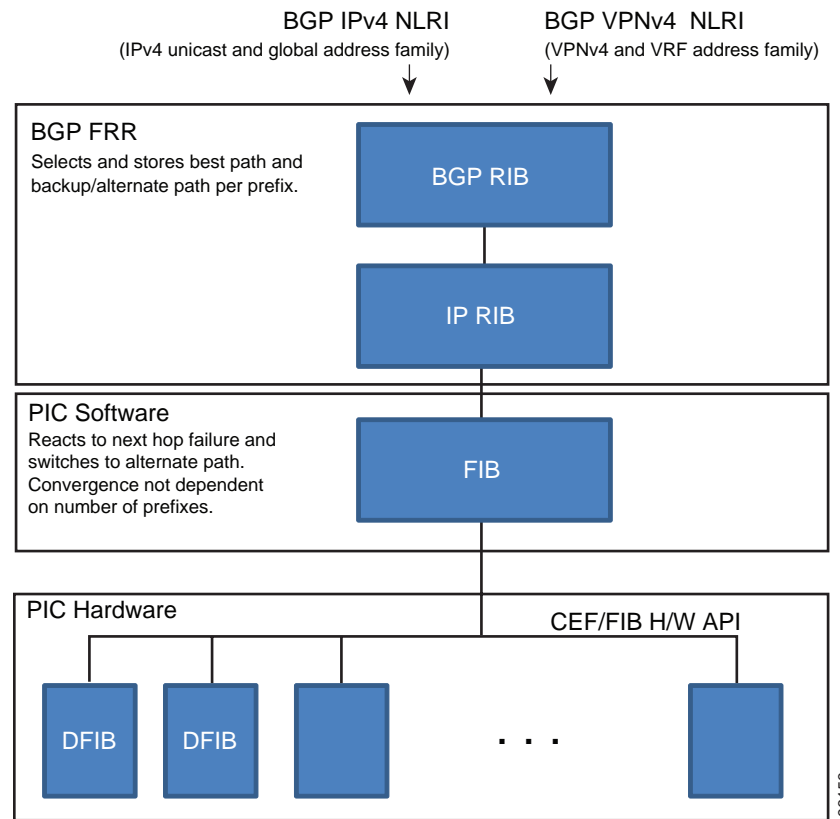
Upon detection of failure, BGP learns about the failure through IGP convergence or BFD events and sends withdraw messages for the prefixes, recalculating the best and backup/alternate paths, and advertising the next best path across the network.

## BGP Fast Reroute's Role in the BGP PIC Feature

BGP Fast Reroute (FRR) provides a best path and a backup/alternate path in BGP, RIB, and Cisco Express Forwarding. BGP FRR provides a very fast reroute mechanism into the RIB and Cisco Express Forwarding on the backup BGP next hop to reach a destination when the current best path is not available.

BGP FRR precomputes a second best path in BGP and gives it to the RIB and Cisco Express Forwarding as a backup/alternate path, and Cisco Express Forwarding programs it into line cards.

Therefore BGP FRR is responsible for the setup of the best path and backup/alternate path. The BGP PIC feature provides the ability for Cisco Express Forwarding to quickly switch the traffic to the other egress ports if the current next hop or the link to this next hop goes down. This is illustrated in [Figure 1](#).

**Figure 1** *BGP PIC Edge and BGP FRR*

196159

## How a Failure Is Detected

If the failure is detected in the IBGP (remote) peer, it is detected by IGP and can take a few seconds for the detection to occur. Convergence can occur in subseconds or seconds, depending on whether PIC is enabled on the line cards.

If the failure is with directly connected neighbors (EBGP), if you use BFD to detect when a neighbor has gone away, the detection is within a subsecond and the convergence can occur in subseconds or seconds, depending on whether PIC is enabled on the line cards.

## How BGP PIC Can Achieve Subsecond Convergence

The BGP PIC feature works at the Cisco Express Forwarding level, and Cisco Express Forwarding can be processed in hardware line cards and in software.

- For platforms that support Cisco Express Forwarding processing in the line cards, the BGP PIC feature can converge in subseconds. The 7600 router supports Cisco Express Forwarding processing in the line cards and thus can attain subsecond convergence.

- For platforms that do not use Cisco Express Forwarding in hardware line cards, Cisco Express Forwarding is achieved in the software. The BGP PIC feature will work with the Cisco Express Forwarding through the software and achieve convergence within seconds. The Cisco 10000 router and the Cisco ASR 1000 series router supports Cisco Express Forwarding in the software and thus can achieve convergence in seconds rather than milliseconds.

## How BGP PIC Improves Upon the Functionality of MPLS VPN—BGP Local Convergence

The BGP PIC feature is an enhancement to the [MPLS VPN—BGP Local Convergence](#) feature, which provides a failover mechanism that recalculates the best path and installs the new path in forwarding after a link failure. The feature maintains the local label for 5 minutes to ensure that the traffic uses the backup/alternate path, thus minimizing traffic loss.

The BGP PIC feature improves the LoC time to under a second by calculating a backup/alternate path in advance. When a link failure occurs, the traffic is sent to the backup/alternate path.

When you configure the BGP PIC feature, it will override the functionality of the [MPLS VPN—BGP Local Convergence](#) feature. You do not have to remove the **protection local-prefixes** command from the configuration.

## Configuration Modes for Enabling BGP PIC

Because many service provider networks contain many VRFs, the BGP PIC feature allows you to configure BGP PIC feature for all VRFs at once.

- VPNv4 address family configuration mode protects all the VRFs.
- VRF-IPv4 address family configuration mode protects only IPv4 VRFs.
- Global router configuration mode protects prefixes in the global routing table.

## BGP PIC Scenarios

The following scenarios explain how you can configure BGP PIC functionality to achieve fast convergence:

- [IP PE–CE Link and Node Protection on the CE Side \(Dual PEs\)](#), page 6
- [IP PE–CE Link and Node Protection on the CE Side \(Dual CEs and Dual PE Primary and Backup Nodes\)](#), page 7
- [IP MPLS PE–CE Link Protection for the Primary or Backup/Alternate Path](#), page 8
- [IP MPLS PE–CE Node Protection for Primary or Backup/Alternate Path](#), page 9

### IP PE–CE Link and Node Protection on the CE Side (Dual PEs)

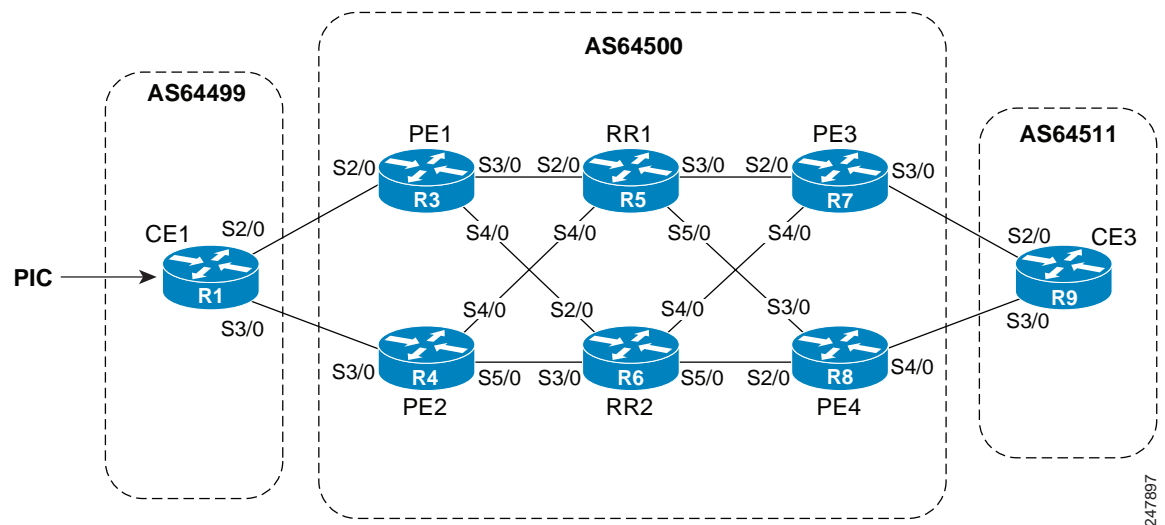
[Figure 2](#) shows a network that uses the BGP PIC feature. The network includes the following components:

- eBGP sessions exist between the PE and CE routers.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through router CE3.

- CE1 has two paths:
  - PE1 as the primary path.
  - PE2 as the backup/alternate path.

CE1 is configured with the BGP PIC feature. BGP computes PE1 as the best path and PE2 as the backup/alternate path and installs both the routes into the RIB and Cisco Express Forwarding forwarding plane. When the CE1–PE1 link goes down, Cisco Express Forwarding detects the link failure and points the forwarding object to the backup/alternate path. Traffic is quickly rerouted due to local fast convergence in Cisco Express Forwarding.

**Figure 2** Using BGP PIC To Protect PE-CE Link



## IP PE–CE Link and Node Protection on the CE Side (Dual CEs and Dual PE Primary and Backup Nodes)

Figure 3 shows a network that uses the BGP PIC feature on CE1. The network includes the following components:

- eBGP sessions exist between the PE and CE routers.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through router CE3.
- CE1 has two paths:
  - PE1 as the primary path.
  - PE2 as the backup/alternate path.
- An iBGP session exists between the CE1 and CE2 routers.

In this example, CE1 and CE2 are configured with the BGP PIC feature. BGP computes PE1 as the best path and PE2 as the backup/alternate path and installs both the routes into the RIB and Cisco Express Forwarding plane.

There should not be any policies set on CE1 and CE2 for the eBGP peers PE1 and PE2. Both CE routers must point to the external eBGP route as next hop. On CE1, the next hop to reach CE3 is through PE1, so PE1 is the best path to reach CE3. On CE2, the best path to reach CE3 is PE2. CE2 advertises to CE1 with itself as the next hop and CE1 does the same to CE2. As a result, CE1 has two paths for the specific

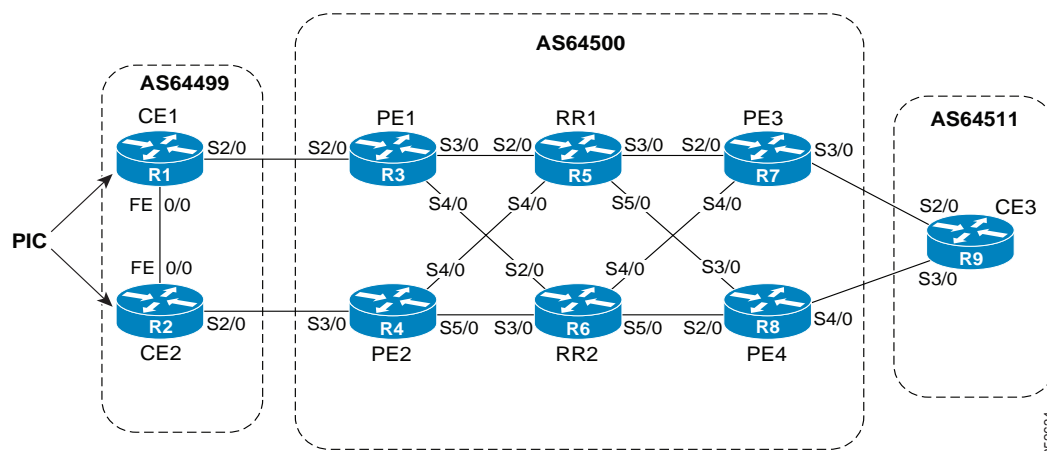


prefix and it usually selects the directly connected eBGP path over the iBGP path through the best path selection rules. Similarly, CE2 has two paths—an eBGP path through PE2 and an iBGP path through CE1–PE1.

When the CE1–PE1 link goes down, Cisco Express Forwarding detects the link failure and points the forwarding object to the backup/alternate node CE2. Traffic is quickly rerouted due to local fast convergence in Cisco Express Forwarding.

If the CE1–PE1 link or PE1 goes down and BGP PIC is enabled on CE1, BGP recomputes the best path, removing the next hop PE1 from RIB and reinstalling CE2 as the nexthop into the RIB and Cisco Express Forwarding. CE1 automatically gets a backup/alternate repair path into Cisco Express Forwarding and the traffic loss during forwarding is now in subseconds, thereby achieving fast convergence.

**Figure 3** Using BGP PIC in a Dual CE, Dual PE Network



## IP MPLS PE–CE Link Protection for the Primary or Backup/Alternate Path

Figure 3 shows a network that uses that uses the BGP PIC feature on CE1 and CE2. The network includes the following components:

- eBGP sessions exist between the PE and CE routers.
- The PE routers are VPNv4 iBGP peers with reflect routers in the MPLS network.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through router CE3.
- CE3 is dual-homed with PE3 and PE4.
- PE1 has two paths to reach CE3 from the reflect routers:
  - PE3 is the primary path with the next hop as a PE3 address.
  - PE4 is the backup/alternate path with the next hop as a PE4 address.

In this example, all the PE routers can be configured with the BGP PIC feature under IPv4 or VPNv4 address families.

For BGP PIC to work in BGP for PE–CE link protection, set the policies on PE3 and PE4 for the prefixes received from CE3 so that one of the PE routers acts as primary and the other as backup/alternate. Usually this is done using local preference and giving better local preference to PE3. In the MPLS cloud, traffic internally flows through PE3 to reach CE3. PE1 thus has PE3 as the best path and PE4 as the second path.

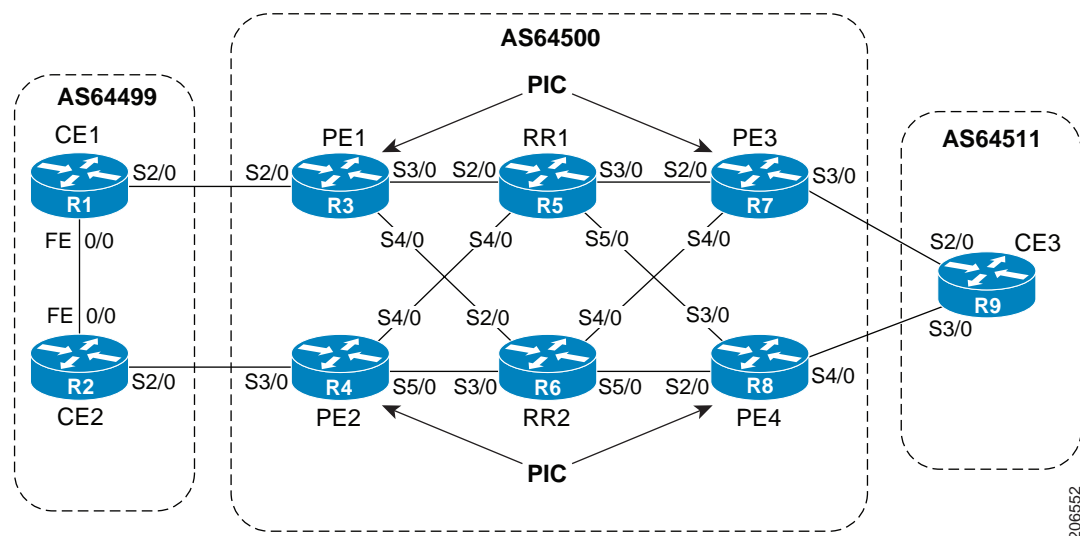
When the PE3–CE3 link goes down, Cisco Express Forwarding detects the link failure, PE3 recomputes the best path and selects PE4 as the best path and sends a withdraw for the PE3 prefix to the reflect routers. Some of the traffic goes through PE3–PE4 until BGP installs PE4 as the best path route into the RIB and Cisco Express Forwarding. PE1 receives the withdraw and recomputes the best path and selects PE4 as the best path and installs the routes into the RIB and Cisco Express Forwarding plane.

Thus, with BGP PIC enabled on PE3 and PE4, Cisco Express Forwarding detects the link failure and does in-place modification of the forwarding object to the backup/alternate node PE4 that already exists in Cisco Express Forwarding. PE4 knows that the backup/alternate path is locally generated and routes the traffic to the egress port connected to CE3. This way, traffic loss is minimized and fast convergence is achieved.

## IP MPLS PE–CE Node Protection for Primary or Backup/Alternate Path

Figure 4 shows a network that uses the BGP PIC feature on all the PE routers in an MPLS network.

**Figure 4** Enabling BGP PIC on All PEs Routers in the MPLS Network



The network includes the following components:

- eBGP sessions exist between the PE and CE routers.
- The PE routers are VPNv4 iBGP peers with reflect routers in the MPLS network.
- Traffic from CE1 uses PE1 to reach network 192.168.9.0/24 through router CE3.
- CE3 is dual-homed with PE3 and PE4.
- PE1 has two paths to reach CE3 from the reflect routers:
  - PE3 is the primary path with the next hop as a PE3 address.
  - PE4 is the backup/alternate path with the next hop as a PE4 address.

In this example, all the PE routers are configured with the BGP PIC feature under IPv4 and VPNv4 address families.

For BGP PIC to work in BGP for the PE–CE node protection, set the policies on PE3 and PE4 for the prefixes received from CE3 such that one of the PE routers acts as primary and the other as backup/alternate. Usually this is done using local preference and giving better local preference to PE3. In the MPLS cloud, traffic internally flows through PE3 to reach CE3. So PE1 has PE3 as the best path and PE4 as the second path.

When PE3 goes down, PE1 knows about the removal of the host prefix by IGP in subseconds and recomputes the best path and selects PE4 as the best path and installs the routes into the RIB and Cisco Express Forwarding forwarding plane. Normal BGP convergence will happen, while BGP PIC is redirecting the traffic through PE4. Thus, packets are not lost.

Thus, with BGP PIC enabled on PE3 Cisco Express Forwarding detects the node failure on PE3 and points the forwarding object to the backup/alternate node PE4. PE4 knows that the backup/alternate path is locally generated and routes the traffic to the egress port using the backup/alternate path. This way, traffic loss is minimized.

#### **No local policies set on the PE routers**

PE1 and PE2 point to the eBGP CE paths as the next hop with no local policy. Each of the PE routers receives the other's path and BGP calculates the backup/alternate path and installs it into Cisco Express Forwarding along with its own eBGP path towards CE as the best path. The limitation of the MPLS PE–CE link and node protection solutions is that you cannot change BGP policies. They should work without the need of a best-external path.

#### **Local policies set on the PE routers**

Whenever there is a local policy on the PE routers to select one of the PE routers as the primary path to reach the egress CE, the `bgp advertise-best-external` command is needed on the backup/alternate node PE3 to propagate the external CE routes with a backup/alternate label into the route reflectors and the far-end PE routers.

## **Cisco Express Forwarding Recursion**

Recursion is the ability to find the next longest matching path when the primary path goes away.

When the BGP PIC feature is not installed, if the next hop to a prefix fails, Cisco Express forwarding finds the next path to reach the prefix by recursing through the FIB to find the next longest matching path to the prefix. This is useful if the next hop is multiple hops away and there is more than one way of reaching the next hop.

However with the of BGP PIC feature, you want to disable Cisco Express Forwarding recursion, for the following reasons:

- Recursion slows down convergence when Cisco Express Forwarding searches all the FIB entries.
- BGP PIC Edge already precomputes an alternate path, thus eliminating the need for CEF recursion.

When BGP PIC functionality is enabled, Cisco Express Forwarding recursion is disabled by default for two conditions :

- For next hops learned with a /32 network mask (host routes)
- For next hops that are directly connected

For all other cases, Cisco Express Forwarding recursion is enabled.

As part of BGP PIC functionality, you can issue the **bgp recursion host** command to disable or enable Cisco Express Forwarding recursion for BGP host routes.

To disable or enable Cisco Express Forwarding recursion for BGP directly connected next hops, you can issue the **disable-connected-check** command.

## How to Configure BGP PIC

Configuring the BGP PIC feature consists of the following task:

- [Enabling BGP PIC, page 11](#)

### Enabling BGP PIC

Because many service provider networks contain many VRFs, the BGP PIC feature allows you to configure BGP PIC feature for all VRFs at once.

- VPNv4 address family configuration mode protects all the VRFs.
- VRF-IPv4 address family configuration mode protects only IPv4 VRFs.
- Global router configuration mode protects prefixes in the global routing table.

For a full configuration example that includes configuring multiprotocol VRFs and show output to verify that the feature is enabled, see the “[Configuring BGP PIC: Example](#)” section on page 13.

### Prerequisites

- If you are implementing the BGP PIC feature in an MPLS VPN, ensure the network is working properly before configuring the BGP PIC feature. See [Configuring MPLS Layer 3 VPNs](#) for more information.
- If you are implementing the BGP PIC feature in an MPLS VPN, configure multiprotocol VRFs, which allows you to share route-targets policies (import and export) between IPv4 and IPv6 or to configure separate route-target policies for IPv4 and IPv6 VPNs. For information on configuring multiprotocol VRFs, see [MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs](#).
- Ensure that the CE router is connected to the network by at least two paths.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **address-family ipv4** [**unicast** | **vrf** *vrf-name*]  
or  
**address-family vpnv4** [**unicast**]
5. **bgp additional-paths install**
6. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
7. **neighbor** *ip-address* **activate**
8. **bgp recursion host**

9. **neighbor ip-address fall-over** [bfd | **route-map** *map-name*]
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router bgp</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 40000                                                                                                                                                         | Enters router configuration mode for the specified routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 4 | <b>address-family ipv4</b> [ <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br>or<br><b>address-family vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 unicast<br>or<br>Router(config-router)# address-family vpnv4 | Specifies the IPv4 or VPNv4 address family and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies the IPv4 or VPNv4 unicast address family.</li> <li>The <b>vrf</b> keyword and <i>vrf-name</i> argument specify the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                   |
| Step 5 | <b>bgp additional-paths install</b><br><br><b>Example:</b><br>Router(config-router-af)# bgp additional-paths install                                                                                                                                                 | Calculates a backup/alternate path and installs it into the RIB and Cisco Express Forwarding.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 6 | <b>neighbor ip-address remote-as</b> <i>autonomous-system-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 remote-as 45000                                                                                                        | Adds the IP address of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>By default, neighbors that are defined using the <b>neighbor remote-as</b> command in router configuration mode exchange only IPv4 unicast address prefixes. To exchange other address prefix types, neighbors must also be activated using the <b>neighbor activate</b> command in address family configuration mode for the other prefix types.</li> </ul> |
| Step 7 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 activate                                                                                                                                                | Enables the neighbor to exchange prefixes for the IPv4 unicast address family with the local router.                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>bgp recursion host</b><br><br><b>Example:</b><br>Router(config-router-af)# bgp recursion host                                                      | (Optional) Enables the recursive-via-host flag for IPv4, VPNv4, and VRF address families. <ul style="list-style-type: none"> <li>When the BGP PIC feature is enabled, Cisco Express Forwarding recursion is disabled. Under most circumstances, you do not want to enable recursion when BGP PIC is enabled.</li> </ul> |
| Step 9  | <b>neighbor ip-address fall-over [bfd  route-map map-name]</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.1.1 fall-over bfd | Enables BFD protocol support to detect when a neighbor has gone away, which can occur within a subsecond.                                                                                                                                                                                                               |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                    | Exits address family configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                |

## Configuration Examples for BGP PIC

The following examples configure and then verify the BGP PIC feature:

- [Configuring BGP PIC: Example, page 13](#)
- [Displaying Backup/Alternate Paths for BGP PIC: Example, page 14](#)

### Configuring BGP PIC: Example

The following example configures the BGP PIC feature in VPNv4 address-family configuration mode, which enables the feature on all VRFs. (The **bgp additional-paths install** command is shown in bold.) In the following example there are two VRFs defined: blue and green. All the VRFs, including those in VRFs blue and green are protected by backup/alternate paths.

```
vrf definition test1
 rd 400:1
 route-target export 100:1
 route-target export 200:1
 route-target export 300:1
 route-target export 400:1
 route-target import 100:1
 route-target import 200:1
 route-target import 300:1
 route-target import 400:1
 address-family ipv4
 exit-address-family
exit
!
interface Ethernet1/0
 vrf forwarding test1
 ip address 10.0.0.1 255.0.0.0
exit
router bgp 3
 no synchronization
```

```

bgp log-neighbor-changes
redistribute static
redistribute connected
neighbor 10.6.6.6 remote-as 3
neighbor 10.6.6.6 update-source Loopback0
neighbor 10.7.7.7 remote-as 3
neighbor 10.7.7.7 update-source Loopback0
no auto-summary
!
address-family vpnv4
  bgp additional-paths install
  neighbor 10.6.6.6 activate
  neighbor 10.6.6.6 send-community both
  neighbor 10.7.7.7 activate
  neighbor 10.7.7.7 send-community both
exit-address-family
!
address-family ipv4 vrf blue
  import path selection all
  import path limit 10
  no synchronization
  neighbor 10.11.11.11 remote-as 1
  neighbor 10.11.11.11 activate
exit-address-family
!
address-family ipv4 vrf green
  import path selection all
  import path limit 10
  no synchronization
  neighbor 10.13.13.13 remote-as 1
  neighbor 10.13.13.13 activate
exit-address-family

```

The following **show vrf detail** command output shows that the BGP PIC feature is enabled. (Relevant output is shown in bold)

```

Router# show vrf detail

VRF test1 (VRF Id = 1); default RD 400:1; default VPNID <not set>
  Interfaces:
    Se4/0
  Address family ipv4 (Table ID = 1 (0x1)):
    Export VPN route-target communities
      RT:100:1          RT:200:1          RT:300:1
      RT:400:1
    Import VPN route-target communities
      RT:100:1          RT:200:1          RT:300:1
      RT:400:1
    No import route-map
    No export route-map
    VRF label distribution protocol: not configured
    VRF label allocation mode: per-prefix
    Prefix protection with additional path enabled
  Address family ipv6 not active.

```

## Displaying Backup/Alternate Paths for BGP PIC: Example

The command output in the following example shows that the VRFs in VRF blue have backup/alternate paths. The relevant command output is shown in bold.

```

Router# show ip bgp vpnv4 vrf blue 10.0.0.0

```

```

BGP routing table entry for 10:12:12.0.0/24, version 88
Paths: (4 available, best #1, table blue)
  Additional-path
    Advertised to update-groups:
      6
    1, imported path from 12:23:12.0.0/24
      10.3.3.3 (metric 21) from 10.6.6.6 (10.6.6.6)
        Origin incomplete, metric 0, localpref 200, valid, internal, best
        Extended Community: RT:12:23
        Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
        mpls labels in/out nolabel/37
    1, imported path from 12:23:12.0.0/24
      10.13.13.13 (via green) from 10.13.13.13 (10.0.0.2)
        Origin incomplete, metric 0, localpref 100, valid, external
        Extended Community: RT:12:23 , recursive-via-connected
    1, imported path from 12:23:12.0.0/24
      10.3.3.3 (metric 21) from 10.7.7.7 (10.7.7.7)
        Origin incomplete, metric 0, localpref 200, valid, internal
        Extended Community: RT:12:23
        Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
        mpls labels in/out nolabel/37
    1
      10.11.11.11 from 10.11.11.11 (1.0.0.1)
        Origin incomplete, metric 0, localpref 100, valid, external, backup/repair
        Extended Community: RT:11:12 , recursive-via-connected

```

The command output in the following example shows that the VRFs in VRF green have backup/alternate paths. The relevant command output is shown in bold.

```
Router# show ip bgp vpnv4 vrf green 12.0.0.0
```

```

BGP routing table entry for 12:23:12.0.0/24, version 87
Paths: (4 available, best #4, table green)
  Additional-path
    Advertised to update-groups:
      5
    1, imported path from 11:12:12.0.0/24
      10.11.11.11 (via blue) from 10.11.11.11 (1.0.0.1)
        Origin incomplete, metric 0, localpref 100, valid, external
        Extended Community: RT:11:12 , recursive-via-connected
    1
      10.3.3.3 (metric 21) from 10.7.7.7 (10.7.7.7)
        Origin incomplete, metric 0, localpref 200, valid, internal
        Extended Community: RT:12:23
        Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
        mpls labels in/out nolabel/37
    1
      10.13.13.13 from 10.13.13.13 (10.0.0.2)
        Origin incomplete, metric 0, localpref 100, valid, external, backup/repair
        Extended Community: RT:12:23 , recursive-via-connected
    1
      10.3.3.3 (metric 21) from 10.6.6.6 (10.6.6.6)
        Origin incomplete, metric 0, localpref 200, valid, internal, best
        Extended Community: RT:12:23
        Originator: 10.3.3.3, Cluster list: 10.0.0.1 , recursive-via-host
        mpls labels in/out nolabel/37

```

The command output in the following example shows the BGP routing table entries for the backup and alternate paths. The relevant command output is shown in bold.

```
Router# show ip bgp 10.0.0.0 255.255.0.0
```

```
BGP routing table entry for 10.0.0.0/16, version 123
```



```

Paths: (4 available, best #3, table default)
Additional-path
Advertised to update-groups:
    2          3
Local
  10.0.101.4 from 10.0.101.4 (10.3.3.3)
    Origin IGP, localpref 100, weight 500, valid, internal
Local
  10.0.101.3 from 10.0.101.3 (10.4.4.4)
    Origin IGP, localpref 100, weight 200, valid, internal
Local
  10.0.101.2 from 10.0.101.2 (10.1.1.1)
    Origin IGP, localpref 100, weight 900, valid, internal, best
Local
  10.0.101.1 from 10.0.101.1 (10.5.5.5)
    Origin IGP, localpref 100, weight 700, valid, internal, backup/repair

```

The command output in the following example shows the routing information base entries for the backup and alternate paths. The relevant command output is shown in bold.

```
Router# show ip route repair-paths 10.0.0.0 255.255.0.0
```

```

Routing entry for 10.0.0.0/16
  Known via "bgp 10", distance 200, metric 0, type internal
  Last update from 10.0.101.2 00:00:56 ago
  Routing Descriptor Blocks:
  * 10.0.101.2, from 10.0.101.2, 00:00:56 ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: none
  [RPR]10.0.101.1, from 10.0.101.1, 00:00:56 ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
    MPLS label: none

```

The command output in the following example shows the Cisco Express Forwarding/forwarding information base entries for the backup and alternate paths. The relevant command output is shown in bold.

```
Router# show ip cef 40.0.0.0 255.255.0.0 detail
```

```

10.0.0.0/16, epoch 0, flags rib only nolabel, rib defined all labels
  recursive via 10.0.101.2
    attached to GigabitEthernet0/2
  recursive via 10.0.101.1, repair
    attached to GigabitEthernet0/2

```

# Additional References

The following sections provide references related to the BGP PIC feature.

## Related Documents

| Related Topic                                                           | Document Title                                          |
|-------------------------------------------------------------------------|---------------------------------------------------------|
| Basic MPLS VPNs                                                         | <a href="#">Configuring MPLS Layer 3 VPNs</a>           |
| A failover feature that creates a new path after a link or node failure | <a href="#">MPLS VPN—BGP Local Convergence</a>          |
| Configuring multiprotocol VRFs                                          | <a href="#">MPLS VPN—VRF CLI for IPv4 and IPv6 VPNs</a> |
| BGP routing                                                             | <a href="#">BGP Feature Roadmap</a>                     |

## Standards

| Standard                          | Title                                                  |
|-----------------------------------|--------------------------------------------------------|
| draft-walton-bgp-add-paths-04.txt | <a href="#">Advertisement of Multiple Paths in BGP</a> |

## MIBs

| MIB | MIBs Link                                                                                                                                                                                                              |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| N/A | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                               |
|----------|-----------------------------------------------------|
| RFC 2547 | <a href="#">BGP/MPLS VPNs</a>                       |
| RFC 1771 | <a href="#">A Border Gateway Protocol 4 (BGP-4)</a> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

## Feature Information for BGP PIC

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1**      **Feature Information for BGP PIC**

| Feature Name                     | Releases                   | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------------|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BGP PIC Edge for IP and MPLS-VPN | 12.2(33)SRE<br>12.2(33)XNE | <p>The BGP PIC feature creates and stores a backup/alternate path in the routing information base (RIB) and in Cisco Express Forwarding, so that in case of a failure, the backup/alternate path can immediately take over, thus enabling subsecond failover.</p> <p>In 12.2(33)SRC, this feature was introduced on the Cisco 7200 router.</p> <p>In 12.2(33)SRB, this feature was introduced on the Cisco 7600 router.</p> <p>In 12.2(33)XNE, support was added for the Cisco 10000 router.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Prerequisites for BGP PIC, page 2</a></li> <li>• <a href="#">Restrictions for BGP PIC, page 2</a></li> <li>• <a href="#">Information About BGP PIC, page 3</a></li> <li>• <a href="#">How to Configure BGP PIC, page 11</a></li> </ul> <p>The following commands were introduced or modified: <b>bgp additional-paths install</b>, <b>bgp recursion host</b>, <b>show ip bgp</b>, <b>show ip route</b>, <b>show ip cef</b>, <b>show vrf</b>.</p> |

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

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

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

© 2009 Cisco Systems, Inc. All rights reserved.





# MPLS VPN—L3VPN over GRE

---

**First Published: September 29, 2008**

**Last Updated: November 20, 2009**

The MPLS VPN—L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network.

The MPLS VPN—L3VPN over GRE feature utilizes MPLS over generic routing encapsulation (MPLSoGRE) to encapsulate MPLS packets inside IP tunnels. This action creates a virtual point-to-point link across non-MPLS networks.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN—L3VPN over GRE”](#) section on page 11.

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

## Contents

- [Prerequisites for MPLS VPN—L3VPN over GRE, page 2](#)
- [Restrictions for MPLS VPN—L3VPN over GRE, page 2](#)
- [Information About MPLS VPN—L3VPN over GRE, page 2](#)
- [How to Configure MPLS VPN—L3VPN over GRE, page 4](#)
- [Configuration Examples for MPLS VPN—L3VPN over GRE, page 6](#)
- [Additional References, page 9](#)
- [Feature Information for MPLS VPN—L3VPN over GRE, page 11](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS VPN—L3VPN over GRE

Before you configure the MPLS VPN—L3VPN over GRE feature, ensure that your MPLS Virtual Private Network (VPN) is configured and working properly. See the [Configuring MPLS Layer 3 VPNs](#) module for information about setting up MPLS VPNs.

Ensure that the following routing protocols are configured and working properly:

- Label Distribution Protocol (LDP)—for MPLS label distribution. See [MPLS Label Distribution Protocol Overview](#).
- Multiprotocol Border Gateway Protocol (MP-BGP)—for VPN route and label distribution. See [Configuring MPLS Layer 3 VPNs](#).

## Restrictions for MPLS VPN—L3VPN over GRE

The MPLS VPN—L3VPN over GRE feature does not support the following:

- Quality of service (QoS) service policies configured on the tunnel interface; they are supported on the physical or subinterface
- GRE options: sequencing, checksum, and source route
- IPv6 GRE
- Advanced features such as Carrier Supporting Carrier (CSC) and Interautonomous System (Inter-AS)

## Information About MPLS VPN—L3VPN over GRE

The MPLS VPN—L3VPN over GRE feature provides a mechanism for tunneling MPLS packets over non-MPLS networks.

MPLS VPN—L3VPN over GRE allows you to create a GRE tunnel across a non-MPLS network. The MPLS packets are encapsulated within the GRE tunnel packets, and the encapsulated packets traverse the non-MPLS network through the GRE tunnel. When GRE tunnel packets are received at the other side of the non-MPLS network, the GRE tunnel packet header is removed and the inner MPLS packet is forwarded to its final destination.

The MPLS VPN—L3VPN over GRE feature supports three GRE tunnel configurations:

- [PE-to-PE Tunneling, page 2](#)
- [P-to-PE Tunneling, page 3](#)
- [P-to-P Tunneling, page 4](#)

## PE-to-PE Tunneling

The provider edge-to-provider edge (PE-to-PE) tunneling configuration provides a scalable way to connect multiple customer networks across a non-MPLS network. With this configuration, traffic that is destined to multiple customer networks is multiplexed through a single GRE tunnel.

**Note**

A similar nonscalable alternative is to connect each customer network through separate GRE tunnels (for example, connecting one customer network for each GRE tunnel).

As shown in [Figure 1](#), the PE routers assign VPN routing and forwarding (VRF) numbers to the customer edge (CE) routers on each side of the non-MPLS network.

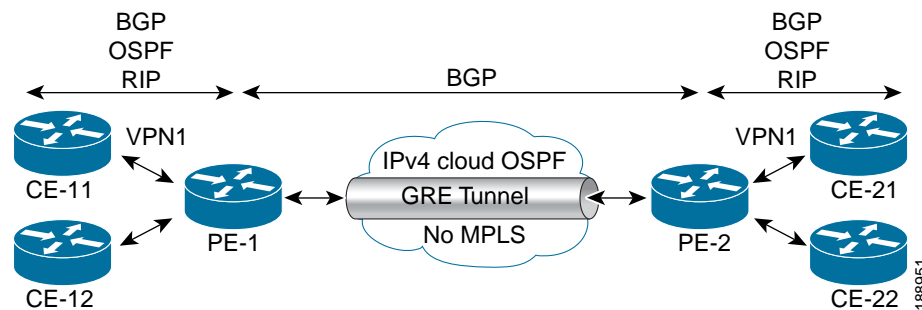
The PE routers use routing protocols such as BGP, OSPF, or Routing Information Protocol (RIP) to learn about the IP networks behind the CE routers. The routes to the IP networks behind the CE routers are stored in the associated CE router's VRF routing table.

The PE router on one side of the non-MPLS network uses the routing protocols (that are operating within the non-MPLS network) to learn about the PE router on the other side of the non-MPLS network. The learned routes that are established between the PE routers are then stored in the main or default routing table.

The opposing PE router uses BGP to learn about the routes that are associated with the customer networks behind the PE routers. These learned routes are not known to the non-MPLS network.

For this example, BGP defines a static route to the BGP neighbor (the opposing PE router) through the GRE tunnel that spans the non-MPLS network. Because the routes that are learned by the BGP neighbor include the GRE tunnel next hop, all customer network traffic is sent using the GRE tunnel.

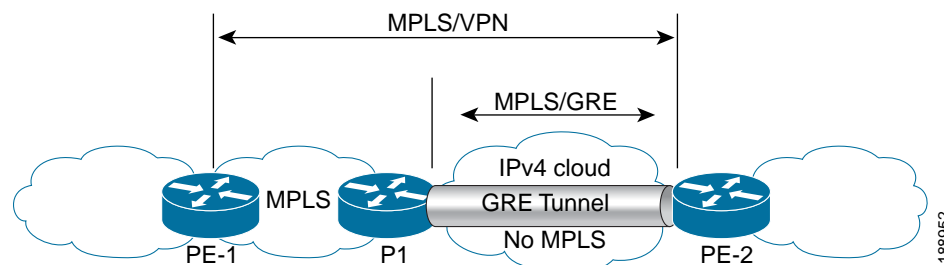
**Figure 1** PE-to-PE Tunneling



## P-to-PE Tunneling

As shown in [Figure 2](#), the provider-to-provider edge (P-to-PE) tunneling configuration provides a way to connect a PE router (P1) to an MPLS segment (PE-2) across a non-MPLS network. In this configuration, MPLS traffic that is destined to the other side of the non-MPLS network is sent through a single GRE tunnel.

**Figure 2** P-to-PE Tunneling

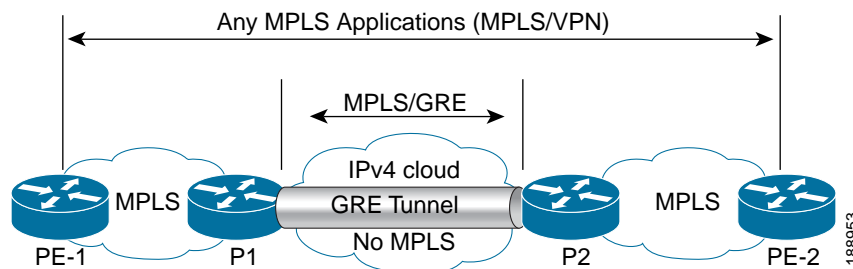




## P-to-P Tunneling

As shown in [Figure 3](#), the provider-to-provider (P-to-P) configuration provides a method of connecting two MPLS segments (P1 to P2) across a non-MPLS network. In this configuration, MPLS traffic that is destined to the other side of the non-MPLS network is sent through a single GRE tunnel.

**Figure 3** P-to-P Tunneling



## How to Configure MPLS VPN—L3VPN over GRE

This section contains the following procedure:

- [Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface, page 4](#) (required)

### Configuring the MPLS VPN—L3VPN over GRE Tunnel Interface

To configure the MPLS VPN—L3VPN over GRE feature, you must create a GRE tunnel to span the non-MPLS networks. You must perform this procedure on the devices located at both ends of the GRE tunnel.

### Prerequisites

Before configuring the MPLS VPN—L3VPN over GRE feature, ensure that your MPLS VPN and the appropriate routing protocols are configured and working properly. See the [“Prerequisites for MPLS VPN—L3VPN over GRE”](#) section on page 2.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *tunnel-number*
4. **ip route** *prefix mask* { *ip-address* | *interface-type interface-number* [*ip-address*] } [**dhcp**] [*distance*] [*name next-hop-name*] [**permanent** | **track** *number*] [**tag** *tag*]
5. **tunnel source** *source-address*
6. **tunnel destination** *destination-address*

7. **mpls ip**
8. **exit**
9. **show ip route**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                                                                                                                      | Enters global configuration mode.                                                                                |
| Step 3 | <b>interface tunnel</b> <i>tunnel-number</i><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                                                                                                                                                                                                                                           | Creates a tunnel on the specified interface and enters interface configuration mode.                             |
| Step 4 | <b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]}</i><br>[ <b>dhcp</b> ] [ <b>distance</b> ] [ <b>name</b> <i>next-hop-name</i> ]<br>[ <b>permanent</b>   <b>track</b> <i>number</i> ] [ <b>tag</b> <i>tag</i> ]<br><br><b>Example:</b><br>Router(config-if)# ip route 209.165.200.253<br>255.255.255.224 FastEthernet 0/0 | Configures a static route to the BGP neighbor on the SIP 2 interface or tunnel interface.                        |
| Step 5 | <b>tunnel source</b> <i>source-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel source<br>209.165.200.254                                                                                                                                                                                                                                            | Specifies the tunnel's source IP address.                                                                        |
| Step 6 | <b>tunnel destination</b> <i>destination-address</i><br><br><b>Example:</b><br>Router(config-if)# tunnel destination<br>209.165.200.255                                                                                                                                                                                                                             | Specifies the tunnel's destination IP address.                                                                   |
| Step 7 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                                                                                                                                                                                                                                                                                 | Enables MPLS on the tunnel's physical interface.                                                                 |

|        | Command or Action                                                            | Purpose                                                                              |
|--------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Step 8 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                | Exits the interface configuration mode.                                              |
| Step 9 | <b>show ip route</b><br><br><b>Example:</b><br>Router(config)# show ip route | Displays the unicast routes and configures a static route globally or on the tunnel. |

## Examples

The following example shows a GRE tunnel configuration that spans a non-MPLS network. This example shows the tunnel configuration on the PE devices (PE1 and PE2) located at both ends of the tunnel:

### PE1 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 209.165.200.253 255.255.255.224
Router(config-if)# tunnel source 209.165.200.254
Router(config-if)# tunnel destination 209.165.200.255
Router(config-if)# mpls ip
```

### PE2 Configuration

```
Router# configure terminal
Router(config)# interface Tunnel 1
Router(config-if)# ip address 209.165.200.235 255.255.255.224
Router(config-if)# tunnel source 209.165.200.240
Router(config-if)# tunnel destination 209.165.200.245
Router(config-if)# mpls ip
```

## Configuration Examples for MPLS VPN—L3VPN over GRE

This section provides the following configuration example for the MPLS VPN—L3VPN over GRE feature:

- [MPLS Configuration with MPLS VPN—L3VPN over GRE: Example, page 6](#)
- [Display of Unicast Routes: Example, page 8](#)

## MPLS Configuration with MPLS VPN—L3VPN over GRE: Example

The following basic MPLS configuration example uses a GRE tunnel to span a non-MPLS network. This example is similar to the configuration shown in [Figure 1 on page 3](#).

### PE1 Configuration

```
!
mpls ip
!
ip vrf vpn1
```

```

rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 209.165.200.225 255.255.255.224
!
interface GigabitEthernet 0/1/2
ip address 209.165.200.226 255.255.255.224
!
interface Tunnel 1
ip address 209.165.200.227 255.255.255.224
tunnel source 209.165.200.228
tunnel destination 209.165.200.229
mpls ip
!
interface GigabitEthernet 0/1/3
ip vrf forwarding vpn1
ip address 209.165.200.230 255.255.255.224
!
router bgp 100
neighbor 209.165.200.231 remote-as 100
neighbor 209.165.200.231 update-source loopback0
!
address-family vpnv4
neighbor 209.165.200.232 activate
neighbor 209.165.200.232 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 209.165.200.240 remote-as 20
neighbor 209.165.200.240 activate
!

```

### PE2 Configuration

```

!
mpls ip
!
ip vrf vpn1
rd 100:1
route-target import 100:1
route-target export 100:1
!
interface loopback 0
ip address 209.165.200.240 255.255.255.224
!
interface GigabitEthernet 0/1/1
ip address 209.165.200.241 255.255.255.224
!
interface Tunnel 1
ip address 209.165.200.244 255.255.255.224
tunnel source 209.165.200.245
tunnel destination 209.165.200.247
mpls ip
!
interface GigabitEthernet 0/0/5
ip vrf forwarding vpn1
ip address 209.165.200.249 255.255.255.224
!
router bgp 100
neighbor 209.165.200.250 remote-as 100
neighbor 209.165.200.252 update-source loopback0
!
address-family vpnv4

```

```

neighbor 209.165.200.253 activate
neighbor 209.165.200.254 send community-extended
!
address-family ipv4 vrf vpn1
neighbor 209.165.200.254 remote-as 30
neighbor 209.165.200.255 activate

```

## Display of Unicast Routes: Example

The following example shows the display of unicast routes. This display shows the next hop for the BGP neighbor depending on the selected interface.

```

Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

    209.165.200.225/32 is subnetted, 1 subnets
O      209.165.200.226 [110/3] via 209.165.200.250, 00:09:55, POS2/0/0
    209.165.200.227/32 is subnetted, 1 subnets
C      209.165.200.229 is directly connected, Loopback0
    209.165.200.230/32 is subnetted, 1 subnets
O      209.165.200.231 [110/2] via 209.165.200.232, 00:09:55, POS2/0/0
S      209.165.200.240/8 [1/0] via 209.165.200.252
    209.165.200.245/32 is subnetted, 2 subnets
S      209.165.200.247 is directly connected, POS2/0/0
O      209.165.200.248 [110/3] via 209.165.200.249, 00:09:55, POS2/0/0
C      209.165.200.254/8 is directly connected, POS2/0/0

```

# Additional References

The following sections provide references related to the MPLS VPN—L3VPN over GRE feature.

## Related Documents

| Related Topic                                                                  | Document Title                                                   |
|--------------------------------------------------------------------------------|------------------------------------------------------------------|
| Setting up MPLS VPN networks<br>Multiprotocol Border Gateway Protocol (MP-BGP) | <a href="#">Configuring MPLS Layer 3 VPNs</a>                    |
| Label Distribution Protocol                                                    | <a href="#">MPLS Label Distribution Protocol Overview</a>        |
| Configuring L3 VPN over mGRE Tunnels                                           | <a href="#">Dynamic Layer-3 VPNs with Multipoint GRE Tunnels</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC  | Title |
|------|-------|
| None | —     |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for MPLS VPN—L3VPN over GRE

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—L3VPN over GRE

| Feature Name                    | Releases                                           | Feature Information                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—L3VPN over GRE feature | 12.0(22)S<br>12.2(13)T<br>12.0(26)S<br>12.2(33)SRE | The MPLS VPN—L3VPN over GRE feature provides a mechanism for tunneling Multiprotocol Label Switching (MPLS) packets over a non-MPLS network.<br><br>This feature uses no new or modified commands. |

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

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

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

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







# Dynamic Layer 3 VPNs with Multipoint GRE Tunnels

---

**First Published: January 23, 2003**

**Last Updated: November 20, 2009**

The Dynamic Layer 3 VPNs with Multipoint GRE Tunnels feature provides a Layer-3 (L3) transport mechanism based on an enhanced multipoint generic routing encapsulation (mGRE) tunneling technology for use in IP networks. The dynamic Layer-3 tunneling transport can also be used within IP networks to transport Virtual Private Network (VPN) traffic across service provider and enterprise networks, and to provide interoperability for packet transport between IP and Multiprotocol Label Switching (MPLS) VPNs. This feature provides support for RFC 2547, which defines the outsourcing of IP backbone services for enterprise networks.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Dynamic L3 VPNs with mGRE Tunnels”](#) section on page 24.

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

## Contents

- [Prerequisites for Dynamic L3 VPNs with mGRE Tunnels, page 2](#)
- [Restrictions for Dynamic L3 VPNs with mGRE Tunnels, page 2](#)
- [Information About Dynamic L3 VPNs with mGRE Tunnels, page 2](#)
- [How to Configure L3 VPN mGRE Tunnels, page 7](#)
- [Configuration Examples for Dynamic L3 VPNs Support Using mGRE Tunnels, page 20](#)



---

**Americas Headquarters:**

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

- [Additional References, page 22](#)
- [Feature Information for Dynamic L3 VPNs with mGRE Tunnels, page 24](#)

## Prerequisites for Dynamic L3 VPNs with mGRE Tunnels

Before you configure the Dynamic Layer 3 VPNs with Multipoint GRE Tunnels feature, ensure that your MPLS VPN is configured and working properly. See the “[Configuring MPLS Layer 3 VPNs](#)” module for information about setting up MPLS VPNs.

## Restrictions for Dynamic L3 VPNs with mGRE Tunnels

- MPLS VPN over mGRE is supported on the Cisco 7600 series routers using the ES-40 line card and the SIP 400 line card as core facing cards.
- Tunnelled tag traffic must enter the router through a line card, which supports MPLS VPN over mGRE. The supported line cards are the ES-40 and the SIP-400.
- The deployment of MPLS VPN using both IP/GRE and MPLS encapsulation within a single network is not supported.
- Each provider edge (PE) router supports one tunnel configuration only.
- MPLS VPN of mGRE does not support the transportation of multicase traffic between VPNs.
- MPLS VPN over mGRE supports a maximum of 4,000 tunnel endpoints per tunnel instance. However, hardware limitations may reduce the number of tunnel endpoints.

## Information About Dynamic L3 VPNs with mGRE Tunnels

You can configure mGRE tunnels to create a multipoint tunnel network that overlays an IP backbone. This overlay connects PE routers to transport VPN traffic.

In addition, when MPLS VPNs are configured over mGRE you can deploy L3 PE-based VPN services using a standards based IP core. This allows you to provision the VPN services without using the overlay method. When MPLS VPN over mGRE is configured, the system uses IPv4-based mGRE tunnels to encapsulate VPN-labeled IPv4 and IPv6 packets between PEs.

This section contains information on the following:

- [Layer 3 mGRE Tunnels, page 2](#)
- [MPLS VPN over mGRE, page 4](#)

## Layer 3 mGRE Tunnels

By configuring mGRE tunnels, you create a multipoint tunnel network as an overlay to the IP backbone. This overlay interconnects the PE routers to transport VPN traffic through the backbone. This multipoint tunnel network uses Border Gateway Protocol (BGP) to distribute VPNv4 routing information between PE routers maintaining the peer relationship between the service provider or enterprise network and customer sites. The advertised next hop in BGP VPNv4 triggers tunnel endpoint discovery. This feature

provides the ability for multiple service providers to cooperate and offer a joint VPN service with traffic tunneled directly from the ingress PE router at one service provider directly to the egress PE router at a different service provider site.

In addition to providing the VPN transport capability, the mGRE tunnels create a full-mesh topology and reduce the administrative and operational overhead previously associated with a full mesh of point-to-point tunnels used to interconnect multiple customer sites. The configuration requirements are greatly reduced and enables the network to grow with minimal additional configuration.

Dynamic L3 tunnels provide for better scaling when creating partial-mesh or full-mesh VPNs. Adding new remote VPN peers is simplified because only the new router needs to be configured. The new address is learned dynamically and propagated to the nodes in the network. The dynamic routing capability dramatically reduces the size of configuration needed on all routers in the VPN, such that with the use of multipoint tunnels, only one tunnel interfaced needs to be configured on a PE that services many VPNs. The L3 mGRE tunnels need to be configured only on the PE router. Features available with GRE are still available with mGRE, including dynamic IP routing and IP multicast and Cisco Express Forwarding (CEF) switching of mGRE/Next Hop Routing Protocol (NHRP) tunnel traffic.

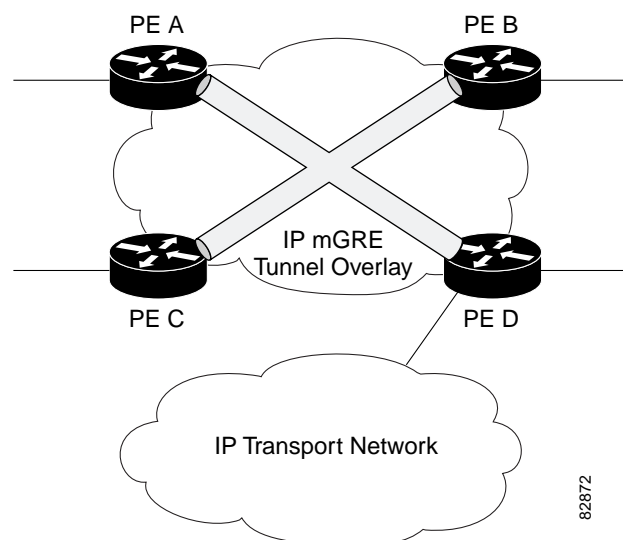
The following sections describe how the mGRE tunnels are used:

- [Interconnecting Provider Edge Routers Within an IP Network, page 3](#)
- [Packet Transport Between IP and MPLS Networks, page 4](#)
- [BGP Next Hop Verification, page 4](#)

## Interconnecting Provider Edge Routers Within an IP Network

The Dynamic Layer 3 VPNs with Multipoint GRE Tunnels feature allows you to create a multi access tunnel network to interconnect the PE routers servicing your IP network. This tunnel network transports IP VPN traffic to all of the PE routers. [Figure 1](#) illustrates the tunnel overlay network used in an IP network to transport VPN traffic between the PE routers.

**Figure 1** mGRE Tunnel Overlay Connecting PE Routers within an IP Network

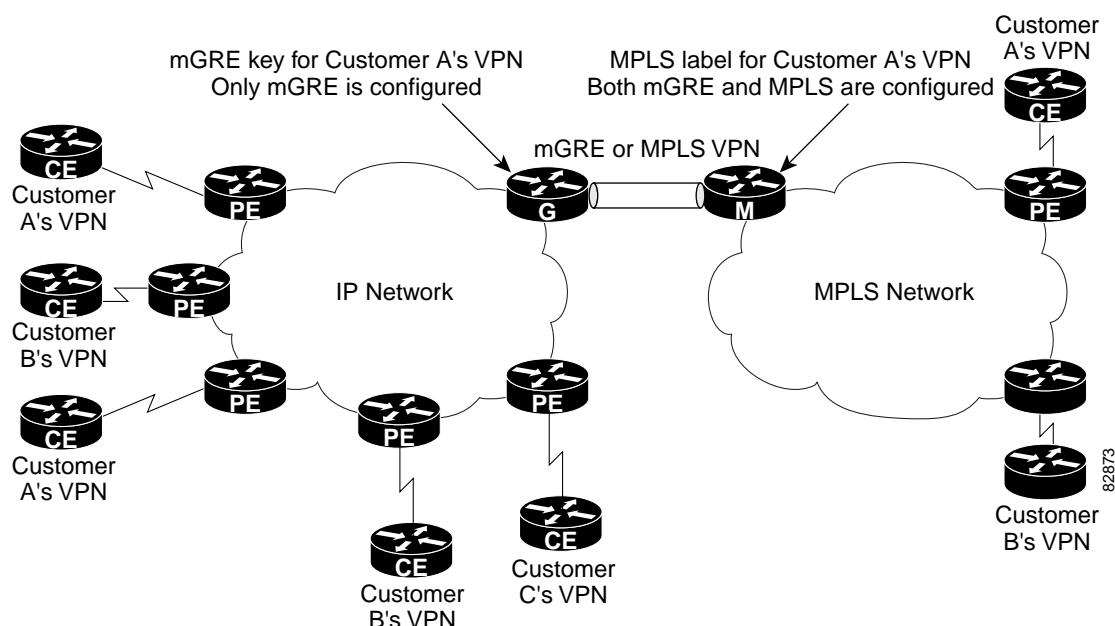


The multi access tunnel overlay network provides full connectivity between PE routers. The PE routers exchange VPN routes using BGP as defined in RFC 2547. IP traffic is redirected through the multipoint tunnel overlay network using distinct IP address spaces for the overlay and transport networks and by changing the address space instead of changing the numerical value of the address.

## Packet Transport Between IP and MPLS Networks

Layer 3 mGRE tunnels can be used as a packet transport mechanism between IP and MPLS networks. To enable the packet transport between the two different protocols, one PE router on one side of the connection between the two networks must run MPLS. [Figure 2](#) shows how mGRE tunnels can be used to transport VPN traffic between PE routers.

**Figure 2** mGRE Used to Transport VPN Traffic Between IP and MPLS Network



For the packet transport to occur between the IP and MPLS network, the MPLS VPN label is mapped to the GRE key. The mapping takes place on the router where both mGRE and MPLS are configured. In [Figure 2](#) the mapping of the label to the key occurs on Router M, which sits on the MPLS network.

## BGP Next Hop Verification

BGP performs the BGP path selection, or next hop verification, at the PE. For a BGP path to a network to be considered in the path selection process, the next hop for the path must be reachable in the Interior Gateway Protocol (IGP). When an IP prefix is received and advertised as the next hop IP address, the IP traffic is tunneled from the source to the destination by switching the address space of the next hop.

## MPLS VPN over mGRE

GRE is a point-to-point tunneling protocol where two peers form the endpoints of the tunnel. It is designed to encapsulate network-layer packets inside IP tunneling packets. mGRE is a similar protocol with a single endpoint at one side of the tunnel connected to multiple endpoints at the other side of the

tunnel. The mGRE tunnel provides a common link between branch offices that connect to the same VPN. As GRE requires a full mesh topology, mGRE uses a point-to-multipoint topology and therefore requires fewer tunnels.

MPLS is a widely deployed VPN internet architecture. MPLS requires that all core routers in the network support MPLS. This feature is useful in networks where the service provider uses a backbone carrier to provide connectivity.

MPLS VPN over mGRE is a feature that overcomes the requirement of the carrier supporting MPLS, by allowing you to provide MPLS connectivity between networks that are connected by IP-only networks. This allows MPLS label switch paths (LSPs) to use GRE tunnels to cross routing areas, autonomous systems and Internet service providers (ISPs).

When MPLS VPNs are configured over mGRE you can deploy L3 Provider Edge (PE) based VPN services using a standards-based IP core. This allows you to provision the VPN services without using LSP or a Label Distribution Protocol (LDP). The system uses IPv4-based mGRE tunnels to encapsulate VPN-labeled IPv4 and IPv6 packets between PEs.

The MPLS VPN over mGRE feature also allows you to deploy existing MPLS VPN LSP-encapsulated technology concurrently with MPLS VPN over mGRE and enables the system to determine which encapsulation method is used to route specific traffic. The ingress PE router determines which encapsulation technology to use when transmitting a packet to the remote PE router.

This section includes information on the following topics:

- [Route Maps, page 6](#)
- [Tunnel Endpoint Discovery and Forwarding, page 6](#)
- [Tunnel Decapsulation, page 6](#)
- [Tunnel Source, page 6](#)
- [IPv6 VPN, page 7](#)

## Route Maps

By default, VPN traffic is sent using an LSP. The MPLS VPN over mGRE feature uses user-defined route-maps to determine which VPN prefixes are reachable over an mGRE tunnel and which VPN prefixes are reachable using an LSP. The route map is applied to advertisements for VPNv4 and VPNv6 address families. The route map uses a NextHOP Tunnel Table to determine the encapsulation method for the VPN traffic.

To route traffic over the mGRE tunnel, the system creates an alternative address space that shows that all next hops are reached by encapsulating the traffic in an mGRE tunnel. To configure a specific route to use an mGRE tunnel, the user adds an entry for that route to the route map. The new entry remaps the Network Layer Reachability Information (NLRI) of the route to the alternative address space. If there is no remap entry in the route map for a route, then traffic on that route is forwarded over an LSP.

When the user configures MPLS VPN over mGRE, the system automatically provisions the alternative address space, normally held in the tunnel-encapsulated virtual routing and forwarding (VRF) instance. To ensure that all traffic reachable through the address space is encapsulated in an mGRE tunnel, the system installs a single default route out of a tunnel. The system also creates a default tunnel on the route map. The user can attach this default route map to the appropriate BGP updates.

## Tunnel Endpoint Discovery and Forwarding

In order for MPLS VPN over mGRE to function correctly, the system must be able to discover the remote PEs in the system and construct tunnel forwarding information for these remote PEs. In addition the system must be able to detect when a remote PE is no longer valid and remove the tunnel forwarding information for that PE.

If an ingress PE receives a VPN advertisement over BGP, it uses the route target attributes (which it inserts into the VRF) and the MPLS VPN label from the advertisement, to associate the prefixes with the appropriate customer. The next hop of the inserted route is set to the NLRI of the advertisement.

The advertised prefixes contain information about remote PEs in the system (in the form of NLRIs), and the PE uses this information to notify the system when an NLRI becomes active or inactive. The system uses this notification to update the PE forwarding information.

When the system receives notification of a new remote PE, it adds the information to the Tunnel Endpoint Database, which causes the system to create an adjacency associated with the tunnel interface. The adjacency description includes information on the encapsulation and other processing that the system must perform to send encapsulated packets to the new remote PE.

The adjacency information is placed into the tunnel encapsulated VRF. When a user remaps a VPN NLRI to a route in the VRF (using the route map) the system links the NLRI to the adjacency, therefore the VPN is linked to a tunnel.

## Tunnel Decapsulation

When the egress PE receives a packet from a tunnel interface that uses MPLS VPN over mGRE, the PE decapsulates the packet to create a VPN label tagged packet, and sends the packet to the MPLS forwarding (MFI) code.

## Tunnel Source

MPLS VPN over mGRE uses a single tunnel configured as a multi point GRE tunnel to configure a system with a large number of endpoints (remote PEs). To identify the origin of tunnel-encapsulated packets, the system uses the tunnel source information.

At the transmitting (ingress) PE, when a VPN packet is sent to a tunnel, the tunnel destination is the NLRI. At a receiving (egress) PE, the tunnel source is the address that the packets encapsulated in the mGRE tunnel are received on. Therefore, at the egress PE the packet destination must match the NLRI from the local PE.

## IPv6 VPN

If the advertising PE router has an IPv6 address then the NLRI must also be an IPv6 address (regardless of the network between the PEs). If the network between the PEs is IPv4 based, the system creates the IPv6 address of the advertising PE using an IPv4 mapped address in the following form: ::FFFF:IPv4-PE-address. The receiving PE sets the next hop for the VPN tag IPv6 prefixes to the IPv4 address embedded in the IPv6 NLRI. This enables the PE to link VPNv6 traffic to an LSP or an mGRE tunnel in the same way it maps VPNv4 traffic.

When a PE receives VPNv6 updates it applies the IPv6 route map. MPLS VPN over mGRE uses the IPv6 route map to set the next hop information in the Tunnel\_Encap VRF.

## How to Configure L3 VPN mGRE Tunnels

To deploy L3 VPN mGRE tunnels you create a VRF instance, create the mGRE tunnel, redirect the VPN IP traffic to the tunnel, and set up the BGP VPNv4 exchange so that updates are filtered through a route map and interesting prefixes are resolved in the VRF table.

To deploy MPLS VPN over mGRE tunnels, you create a VRF instance, enable and configure L3 VPN encapsulation, link the route map to the application template, and set up the BGP VPNv4 and VPNv6 exchange so that updates are filtered through the route map.

The configuration steps to deploy MPLS VPN over mGRE are described in the following sections:

- [Creating the VRF and mGRE Tunnel, page 7](#) (Required)
- [Setting Up BGP VPN Exchange, page 9](#) (Required)
- [Enabling the MPLS VPN over mGRE Tunnels and Configuring L3VPN Encapsulation Profile, page 11](#) (Required)
- [Defining the Address Space and Specifying Address Resolution for MPLS VPNs over mGRE, page 14](#) (Required)

## Creating the VRF and mGRE Tunnel

The tunnel that transports the VPN traffic across the service provider network resides in its own address space. A special VRF instance must be created called Resolve in VRF (RiV). This section describes how to create the VRF and GRE tunnel.

### Prerequisites

The IP address on the interface should be the same as that of the source interface specified in the configuration. The source interface specified should match that used by BGP as a source for the VPNv4 update.



### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf *vrf-name***
4. **rd 1:1**
5. **interface tunnel *tunnel name***
6. **ip address *ip-address subnet-id***
7. **tunnel source loopback *n***
8. **tunnel mode gre multipoint l3vpn**
9. **tunnel key *gre-key***
10. **end**

### DETAILED STEPS

|        | Command or Action                                                                                                                    | Purpose                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                       | Enters global configuration mode.                                                                                                   |
| Step 3 | <b>ip vrf <i>vrf-name</i></b><br><br><b>Example:</b><br>Router(config)# ip vrf customer a riv                                        | Creates the special Resolve in VRF (RiV) VRF instance and table that will be used for the tunnel and redirection of the IP address. |
| Step 4 | <b>rd 1:1</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 1:1                                                                   | Enters the VRF configuration mode and specifies a route distinguisher (RD) for a VPN VRF instance.                                  |
| Step 5 | <b>interface tunnel <i>tunnel name</i></b><br><br><b>Example:</b><br>Router(config-vrf)# interface tunnel 1                          | Enters interface configuration mode to create the tunnel.                                                                           |
| Step 6 | <b>ip address <i>ip-address subnet-id</i></b><br><br><b>Example:</b><br>Router(config-if)# ipaddress 209.165.200.225 255.255.255.224 | Specifies the IP address for the tunnel.                                                                                            |

|         | Command or Action                                                                                                           | Purpose                                                                   |
|---------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Step 7  | <code>tunnel source loopback <i>n</i></code><br><br><b>Example:</b><br>Router(config-if)# tunnel source loopback test1      | Creates the loopback interface.                                           |
| Step 8  | <code>tunnel mode gre multipoint l3vpn</code><br><br><b>Example:</b><br>Router(config-if)# tunnel mode gre multipoint l3vpn | Sets the mode for the tunnel as “gre multipoint l3vpn”.                   |
| Step 9  | <code>tunnel key gre-key</code><br><br><b>Example:</b><br>Router(config-if)# tunnel key 18                                  | Specifies the GRE key for the tunnel.                                     |
| Step 10 | <code>end</code><br><br><b>Example:</b><br>Router(config-if)# end                                                           | Exits the current configuration mode and returns to privileged EXEC mode. |

## Setting Up BGP VPN Exchange

The configuration task described in this section sets up the BGP VPNv4 exchange so that the updates are filtered through a route map and interesting prefixes are resolved in the VRF table.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel tunnel name`
4. `ip route vrf rv-vrf-name IP address subnet mask tunnel n`
5. `router bgp as-number`
6. `network network id`
7. `neighbor {ip-address | peer-group-name} remote-as as-number`
8. `neighbor {ip-address | peer-group-name} update-source interface-type`
9. `address-family vpnv4 [unicast]`
10. `neighbor {ip-address | peer-group-name} activate`
11. `neighbor {ip-address | peer-group-name} route-map map-name {in | out}`
12. `set ip next-hop resolve-in-vrf vrf name`
13. `end`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                               | Enters global configuration mode.                                                                                                           |
| Step 3 | <b>interface tunnel tunnel name</b><br><br><b>Example:</b><br>Router(config)# interface tunnel 1                                                                             | Enters interface configuration mode for the tunnel.                                                                                         |
| Step 4 | <b>ip route vrf riv-vrf-name ip address subnet mask tunnel n</b><br><br><b>Example:</b><br>Router(config-if)# ip route vrf 209.165.200.226 255.255.255.224 tunnel 1          | Sets the packet forwarding to the special RiV VRF.                                                                                          |
| Step 5 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                         | Specifies the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. |
| Step 6 | <b>network network id</b><br><br><b>Example:</b><br>Router(config)# network 209.165.200.255                                                                                  | Specifies the network ID for the networks to be advertised by the BGP and multiprotocol BGP routing processes.                              |
| Step 7 | <b>neighbor {ip-address   peer-group-name} remote-as as-number</b><br><br><b>Example:</b><br>Router(config)# neighbor 209.165.200.227 remote-as 100                          | Adds an entry to the BGP or multiprotocol BGP neighbor table.                                                                               |
| Step 8 | <b>neighbor {ip-address   peer-group-name} update-source interface-type</b><br><br><b>Example:</b><br>Router(config)# neighbor 209.165.200.228 update-source FastEthernet0/1 | Specifies a specific operational interface that BGP sessions use for TCP connections.                                                       |
| Step 9 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config)# address-family vpnv4                                                                         | Specifies address family configuration mode for configuring routing sessions, such as BGP, that use standard VPN4 address prefixes.         |

|         | Command or Action                                                                                                                                                                                                    | Purpose                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config)# neighbor 209.165.200.229<br>activate                                                     | Enables the exchange of information with a neighboring router.                                                                         |
| Step 11 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>route-map</b> <i>map-name</i> { <b>in</b>   <b>out</b> }<br><br><b>Example:</b><br>Router(config)# neighbor 209.165.200.230<br>route-map mpt in | Applies a route map to incoming or outgoing routes. <ul style="list-style-type: none"> <li>Use once for each inbound route.</li> </ul> |
| Step 12 | <b>set ip next-hop resolve-in-vrf</b> <i>vrf name</i><br><br><b>Example:</b><br>Router(config)# set ip next-hop resolve-in-vrf<br>vrft                                                                               | Specifies that the next hop is to be resolved in the VRF table for the specified VRF.                                                  |
| Step 13 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                             | Exits the current configuration mode and returns to privileged EXEC mode.                                                              |

## Enabling the MPLS VPN over mGRE Tunnels and Configuring L3VPN Encapsulation Profile

This section describes how to define the VRF, enable MPLS VPN over mGRE, and configure an L3VPN encapsulation profile.



### Note

Transport protocols such as IPv6, MPLS, IP, and Layer 2 Tunneling Protocol version 3 (L2TPv3) can also be used in this configuration.

## Prerequisites

To enable and configure MPLS VPN over mGRE you must first define the VRF for tunnel encapsulation and enable L3VPN encapsulation in the system.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd 1:1**

5. **exit**
6. **ip cef**
7. **ipv6 unicast-routing**
8. **ipv6 cef**
9. **l3vpn encapsulation ip** *profile name*
10. **transport ipv4** [*source interface n*]
11. **protocol gre** [*key gre-key*]
12. **exit**
13. **interface** *type number*
14. **ip address** *ip-address mask*
15. **ip router isis**
16. **end**

## DETAILED STEPS

|        | Command or Action                                                                                           | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                              | Enters global configuration mode.                                                                                |
| Step 3 | <b>vrf definition</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# vrf definition tunnel encap | Configures a VPN VRF routing table instance and enters VRF configuration mode.                                   |
| Step 4 | <b>rd</b> 1:1<br><br><b>Example:</b><br>Router(config-vrf)# rd 1:1                                          | Specifies an RD for a VPN VRF instance.                                                                          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# exit                                              | Exits VRF configuration mode.                                                                                    |
| Step 6 | <b>ip cef</b><br><br><b>Example:</b><br>Router(config)# ip cef                                              | Enables Cisco Express Forwarding on the router.                                                                  |

|         | Command or Action                                                                                                                        | Purpose                                                                                                                                                              |
|---------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <code>ipv6 unicast-routing</code><br><br><b>Example:</b><br>Router(config)# ipv6 unicast-routing                                         | Enables the forwarding of IPv6 unicast datagrams.                                                                                                                    |
| Step 8  | <code>ipv6 cef</code><br><br><b>Example:</b><br>Router(config)# ipv6 cef                                                                 | Enables Cisco Express Forwarding for IPv6 on the router.                                                                                                             |
| Step 9  | <code>l3vpn encapsulation ip profile name</code><br><br><b>Example:</b><br>Router(config)# l3vpn encapsulation ip tunnel encap           | Enters L3 VPN encapsulation configuration mode to create the tunnel.                                                                                                 |
| Step 10 | <code>transport ipv4 source interface n</code><br><br><b>Example:</b><br>Router(config-l3vpn-encap-ip)# transport ipv4 source loopback 0 | Specifies IPv4 transport source mode and defines the transport source interface.                                                                                     |
| Step 11 | <code>protocol gre [key gre-key]</code><br><br><b>Example:</b><br>Router(config-l3vpn-encap-ip)# protocol gre key 1234                   | Specifies GRE as the tunnel mode and sets the GRE key.                                                                                                               |
| Step 12 | <code>exit</code><br><br><b>Example:</b><br>Router(config-l3vpn-encap-ip)# exit                                                          | Exits L3 VPN encapsulation configuration mode.                                                                                                                       |
| Step 13 | <code>interface type number</code><br><br><b>Example:</b><br>Router(config)# interface loopback 0                                        | Enters interface configuration mode to configure the interface type.                                                                                                 |
| Step 14 | <code>ip address ip-address mask</code><br><br><b>Example:</b><br>Router(config-if)# ip address 10.10.10.4 255.255.255.255               | Specifies the primary IP address and mask for the interface.                                                                                                         |
| Step 15 | <code>ip router isis</code><br><br><b>Example:</b><br>Router(config-if)# ip router isis                                                  | Configures an Intermediate System-to-Intermediate System (IS-IS) routing process for IP on the interface and attaches a null area designator to the routing process. |
| Step 16 | <code>end</code><br><br><b>Example:</b><br>Router(config-if)#end                                                                         | Exits the current configuration mode and returns to privileged EXEC mode.                                                                                            |

## Defining the Address Space and Specifying Address Resolution for MPLS VPNs over mGRE

This section describes how to define the address space and specify the address resolution for MPLS VPNs over mGRE. The following steps also enables you to link the route map to the application template and sets up the BGP VPNv4 and VPNv6 exchange so that updates are filtered through the route map.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** *ip-address* **remote-as** *as-number*
6. **neighbor** *ip-address* **update-source** *interface name*
7. **address-family ipv4**
8. **no synchronization**
9. **redistribute connected**
10. **neighbor** *ip-address* **activate**
11. **no auto-summary**
12. **exit**
13. **address-family vpnv4**
14. **neighbor** *ip-address* **activate**
15. **neighbor** *ip-address* **send-community both**
16. **neighbor** *ip-address* **route-map** *map-name* **in**
17. **exit**
18. **address-family vpnv6**
19. **neighbor** *ip-address* **activate**
20. **neighbor** *ip-address* **send-community both**
21. **neighbor** *ip-address* **route-map** *map-name* **in**
22. **exit**
23. **route-map** *map-tag* **permit** *position*
24. **set ip next-hop encapsulate l3vpn** *profile name*
25. **set ipv6 next-hop encapsulate l3vpn** *profile name*
26. **exit**
27. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                      | Purpose                                                                                                                                                                                                                                             |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                         | Enters global configuration mode.                                                                                                                                                                                                                   |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router (config)# router bgp 100                                                                  | Specifies the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along and enters router configuration mode.                                                                    |
| Step 4 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router (config-router)# bgp log-neighbor-changes                                             | Enables logging of BGP neighbor resets.                                                                                                                                                                                                             |
| Step 5 | <b>neighbor ip-address remote-as as-number</b><br><br><b>Example:</b><br>Router (config-router)# neighbor 10.10.10.6 remote-as 100                     | Adds an entry to the BGP or multiprotocol BGP neighbor table.                                                                                                                                                                                       |
| Step 6 | <b>neighbor ip-address update-source interface name</b><br><br><b>Example:</b><br>Router (config-router)# neighbor 10.10.10.6 update-source loopback 0 | Allows BGP sessions to use any operational interface for TCP connections.                                                                                                                                                                           |
| Step 7 | <b>address-family ipv4</b><br><br><b>Example:</b><br>Router (config-router)# address-family vpv4                                                       | Enters address family configuration mode to configure routing sessions, that use IPv4 address prefixes.                                                                                                                                             |
| Step 8 | <b>no synchronization</b><br><br><b>Example:</b><br>Router (config-router-af)# no synchronization                                                      | Enables the Cisco IOS software to advertise a network route without waiting for an IGP.                                                                                                                                                             |
| Step 9 | <b>redistribute connected</b><br><br><b>Example:</b><br>Router (config-router-af)# redistribute connected                                              | Redistributes routes from one routing domain into another routing domain and allows the target protocol to redistribute routes learned by the source protocol and connected prefixes on those interfaces over which the source protocol is running. |



|         | Command or Action                                                                                                                                              | Purpose                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router (config-router-af)# neighbor 10.10.10.6 activate                                          | Enables the exchange of information with a BGP neighbor.                                                                       |
| Step 11 | <b>no auto-summary</b><br><br><b>Example:</b><br>Router (config-router-af)# no auto-summary                                                                    | Disables automatic summarization and sends subprefix routing information across classful network boundaries                    |
| Step 12 | <b>exit</b><br><br><b>Example:</b><br>Router (config-router-af)# exit                                                                                          | Exits address family configuration mode.                                                                                       |
| Step 13 | <b>address-family vpnv4</b><br><br><b>Example:</b><br>Router (config-router)# address-family vpnv4                                                             | Enters address family configuration mode to configure routing sessions, such as BGP, that use standard VPNv4 address prefixes. |
| Step 14 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router (config-router-af)# neighbor 10.10.10.6 activate                                          | Enables the exchange of information with a BGP neighbor.                                                                       |
| Step 15 | <b>neighbor ip-address send-community both</b><br><br><b>Example:</b><br>Router (config-router-af)# neighbor 10.10.10.6 send-community both                    | Specifies that a communities attribute, for both standard and extended communities, should be sent to a BGP neighbor.          |
| Step 16 | <b>neighbor ip-address route-map map-name in</b><br><br><b>Example:</b><br>Router (config-router-af)# neighbor 10.10.10.6 route-map SELECT UPDATE FOR L3VPN in | Applies the named route map to the incoming route.                                                                             |
| Step 17 | <b>exit</b><br><br><b>Example:</b><br>Router (config-router-af)# exit                                                                                          | Exits address family configuration mode.                                                                                       |
| Step 18 | <b>address-family vpnv6</b><br><br><b>Example:</b><br>Router (config-router)# address-family vpnv4                                                             | Enters address family configuration mode to configure routing sessions, such as BGP, that use VPNv6 address prefixes.          |
| Step 19 | <b>neighbor ip-address activate</b><br><br><b>Example:</b><br>Router (config-router-af)# neighbor 209.165.200.252 activate                                     | Enables the exchange of information with a BGP neighbor.                                                                       |

|         | Command or Action                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 20 | <pre>neighbor ip-address send-community both</pre> <p><b>Example:</b><br/> Router (config-router-af)# neighbor<br/> 209.165.200.252 send-community both </p>                           | Specifies that a communities attribute, for both standard and extended communities, should be sent to a BGP neighbor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 21 | <pre>neighbor ip-address route-map ip-address in</pre> <p><b>Example:</b><br/> Router (config-router-af)# neighbor<br/> 209.165.200.252 route-map SELECT UPDATE FOR<br/> L3VPN in </p> | Applies the named route map to the incoming route.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 22 | <pre>exit</pre> <p><b>Example:</b><br/> Router (config-router-af)# exit </p>                                                                                                           | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 23 | <pre>route-map map-tag permit position</pre> <p><b>Example:</b><br/> Router (config-router)# route-map SELECT UPDATE<br/> FOR L3VPN permit 10 </p>                                     | <p>Enters route-map configuration mode and defines the conditions for redistributing routes from one routing protocol into another.</p> <ul style="list-style-type: none"> <li>• The <b>redistribute</b> router configuration command uses the specified map tag to reference this route map. Multiple route maps may share the same map tag name.</li> <li>• If the match criteria are met for this route map, the route is redistributed as controlled by the set actions.</li> <li>• If the match criteria are not met, the next route map with the same map tag is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.</li> <li>• The <i>position</i> argument indicates the position a new route map will have in the list of route maps already configured with the same name.</li> </ul> |
| Step 24 | <pre>set ip next-hop encapsulate l3vpn tunnel encap</pre> <p><b>Example:</b><br/> Router (config-route-map)# set ip next-hop<br/> encapsulate l3vpn my profile </p>                    | Indicates that output IPv4 packets that pass a match clause of the route map are sent to the VRF for tunnel encapsulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 25 | <pre>set ipv6 next-hop encapsulate l3vpn profile<br/>name</pre> <p><b>Example:</b><br/> Router (config-route-map)# set ip next-hop<br/> encapsulate l3vpn tunnel encap </p>            | Indicates that output IPv6 packets that pass a match clause of the route map are sent to the VRF for tunnel encapsulation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|         | Command or Action                                               | Purpose                                                                  |
|---------|-----------------------------------------------------------------|--------------------------------------------------------------------------|
| Step 26 | <code>exit</code>                                               | Exits route-map configuration mode and enters global configuration mode. |
|         | <b>Example:</b><br>Router (config-route-map)# <code>exit</code> |                                                                          |
| Step 27 | <code>exit</code>                                               | Exits global configuration mode.                                         |
|         | <b>Example:</b><br>Router (config)# <code>exit</code>           |                                                                          |

## What to Do Next

You can perform the following to make sure that the configuration is working properly.

### Check the VRF Prefix

Verify that the specified VRF prefix has been received by BGP. The BGP table entry should show that the route map has worked and that the next hop is showing in the RiV. Use the **show ip bgp vpnv4** command as shown in this example:

```
Router# show ip bgp vpnv4 vrf customer 209.165.200.250
BGP routing table entry for 100:1:209.165.200.250/24, version 12
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
209.165.200.251 in "my riv" from 209.165.200.251 (209.165.200.251)
  Origin incomplete, metric 0, localpref 100, valid, internal, best
  Extended Community: RT:100:1
```

Confirm that the same information has been propagated to the routing table:

```
Router# show ip route vrf customer 209.165.200.250
Routing entry for 209.165.200.250/24
  Known via "bgp 100", distance 200, metric 0, type internal
  Last update from 209.165.200.251 00:23:07 ago
  Routing Descriptor Blocks:
  * 209.165.200.251 (my riv), from 209.165.200.251, 00:23:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 0
```

### CEF Switching

You can also verify that CEF switching is working as expected:

```
Router# show ip cef vrf customer 209.165.200.250
209.165.200.250/24, version 6, epoch 0
0 packets, 0 bytes
  tag information set
    local tag: VPN-route-head
    fast tag rewrite with Tu1, 123.1.1.2, tags imposed: {17}
  via 209.165.200.251, 0 dependencies, recursive
    next hop 209.165.200.251, Tunnel1 via 209.165.200.251/32 (my riv)
    valid adjacency
    tag rewrite with Tu1, 209.165.200.251, tags imposed: {17}
```

## Endpoint Creation

Note that in this example display the tunnel endpoint has been created correctly:

```
Router# show tunnel endpoint tunnel 1
Tunnell running in multi-GRE/IP mode
RFC2547/L3VPN Tunnel endpoint discovery is active on Tu1
Transporting l3vpn traffic to all routes recursing through "my riv"

Endpoint 209.165.200.251 via destination 209.165.200.251
Endpoint 209.165.200.254 via destination 209.165.200.254
```

## Adjacency

Confirm that the corresponding adjacency has been created.

```
Router# show adjacency Tunnel 1 interface
Protocol Interface      Address
TAG       Tunnell          209.165.200.251(4)
                                15 packets, 1980 bytes
                                4500000000000000FF2FC3C77B010103
                                7B01010200008847
                                Epoch: 0
                                Fast adjacency disabled
                                IP redirect disabled
                                IP mtu 1472 (0x0)
                                Fixup enabled (0x2)
                                GRE tunnel
                                Adjacency pointer 0x624A1580, refCount 4
                                Connection Id 0x0
                                Bucket 121
```

Note that because MPLS is being transported over mGRE, the LINK\_TAG adjacency is the relevant adjacency. The MTU reported in the adjacency is the payload length (including the MPLS label) that the packet will accept. The mac string shown in the adjacency display can be interpreted as follows:

```
45000000 -> Beginning of IP Header (Partially populated, t1 & chksum
00000000   are fixed up per packet)
FF2FC3C7
7B010103 -> Source IP Address in transport network 209.165.200.253
7B010102 -> Destination IP address in transport network 209.165.200.252
00008847 -> GRE Header
```

Refer to the [Cisco IOS Multiprotocol Label Switching Configuration Guide](#) for information about configuring MPLS Layer 3 VPNs.

You can use **show l3vpn encapsulation profile name** command to get information on the basic state of the application. The output of this command provides you details on the references to the tunnel and VRF.

# Configuration Examples for Dynamic L3 VPNs Support Using mGRE Tunnels

This section provides an example to configure the layer 3 VPN over mGRE.

- [Configuring Layer 3 VPN mGRE Tunnels: Example, page 20](#)

## Configuring Layer 3 VPN mGRE Tunnels: Example

This example shows the configuration sequence for creating mGRE tunnels. It includes the definition of the special VRF instance.

```
ip vrf my riv
  rd 1:1
interface Tunnell
  ip vrf forwarding my_riv
  ip address 209.165.200.250 255.255.255.224
  tunnel source Loopback0
  tunnel mode gre multipoint l3vpn
  tunnel key 123
end
ip route vrf my riv ip address subnet mask Tunnell

router bgp 100
  network 209.165.200.251
  neighbor 209.165.200.250 remote-as 100
  neighbor 209.165.200.250 update-source Loopback0
  !
  address-family vpnv4
  neighbor 209.165.200.250 activate
  neighbor 209.165.200.250 route-map SELECT_UPDATES_FOR_L3VPN_OVER_MGRE in
  !
  route-map SELECT_UPDATES_FOR_L3VPN_OVER_MGRE permit 10
  set ip next-hop in-vrf my riv
```

This example shows the configuration to link a route map to the application:

```
vrf definition Customer A
  rd 100:110
  route-target export 100:1000
  route-target import 100:1000
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
vrf definition tunnel encap
  rd 1:1
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
  !
ip cef
```

```
!
ipv6 unicast-routing
ipv6 cef
!
!
l3vpn encapsulation ip profile name
  transport source loopback 0
  protocol gre key 1234
!
!
interface Loopback0
  ip address 209.165.200.252 255.255.255.224
  ip router isis
!
interface Serial2/0
  vrf forwarding Customer A
  ip address 209.165.200.253 255.255.255.224
  ipv6 address 3FFE:1001::/64 eui-64
  no fair-queue
  serial restart-delay 0
!
router bgp 100
  bgp log-neighbor-changes
  neighbor 209.165.200.254 remote-as 100
  neighbor 209.165.200.254 update-source Loopback0
  !
  address-family ipv4
    no synchronization
    redistribute connected
    neighbor 209.165.200.254 activate
    no auto-summary
  exit-address-family
  !
  address-family vpnv4
    neighbor 209.165.200.254 activate
    neighbor 209.165.200.254 send-community both
    neighbor 209.165.200.254 route-map SELECT UPDATE FOR L3VPN in
  exit-address-family
  !
  address-family vpnv6
    neighbor 209.165.200.254 activate
    neighbor 209.165.200.254 send-community both
    neighbor 209.165.200.254 route-map SELECT UPDATE FOR L3VPN in
  exit-address-family
  !
  address-family ipv4 vrf Customer A
    no synchronization
    redistribute connected
  exit-address-family
  !
  address-family ipv6 vrf Customer A
    redistribute connected
    no synchronization
  exit-address-family
  !
  !
  route-map SELECT UPDATE FOR L3VPN permit 10
  set ip next-hop encapsulate <profile_name>
  set ipv6 next-hop encapsulate <profile_name>
```

# Additional References

For additional information related to dynamic L3 VPN mGRE tunnels, refer to the following references:

## Related Documents

| Related Topic                 | Document Title                                                                 |
|-------------------------------|--------------------------------------------------------------------------------|
| Configuring MPLS Layer 3 VPNs | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a>    |
| Cisco Express Forwarding      | <a href="#">Cisco IOS IP Switching Configuration Guide</a>                     |
| Generic Routing Encapsulation | <a href="#">Cisco IOS Interface and Hardware Component Configuration Guide</a> |

## Standards

| Standard | Title |
|----------|-------|
| None     | —     |

## MIBs

| MIB                     | MIBs Link                                                                                                                                                                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IETF-PPVPN-MPLS-VPN-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                            |
|----------|------------------------------------------------------------------|
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                             |
| RFC 2784 | <i>Generic Routing Encapsulation (GRE)</i>                       |
| RFC 2890 | <i>Key Sequence Number Extensions to GRE</i>                     |
| RFC 4023 | <i>Encapsulating MPLS in IP or Generic Routing Encapsulation</i> |
| RFC 4364 | <i>BGP/MPLS IP Virtual Private Networks (VPNs)</i>               |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |



# Feature Information for Dynamic L3 VPNs with mGRE Tunnels

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(23)S or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Dynamic L3 VPNs with mGRE Tunnels

| Feature Name                                                                       | Releases    | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dynamic Layer-3 VPNs (L3 VPNs) (RFC 2547 based) with Multipoint GRE (mGRE) Tunnels | 12.0(23)S   | This feature provides an L3 transport mechanism based on an enhanced mGRE tunneling technology for use in IP networks.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| MPLS VPN over mGRE                                                                 | 12.2(33)SRE | <p>This feature provides support to carry MPLS Layer 3 VPN traffic over mGRE. This feature also supports SIP400 and ES40 on Cisco 7600 series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Layer 3 mGRE Tunnels, page 2</a></li> <li>• <a href="#">MPLS VPN over mGRE, page 4</a></li> <li>• <a href="#">Creating the VRF and mGRE Tunnel, page 7</a></li> <li>• <a href="#">Setting Up BGP VPN Exchange, page 9</a></li> <li>• <a href="#">Enabling the MPLS VPN over mGRE Tunnels and Configuring L3VPN Encapsulation Profile, page 11</a></li> <li>• <a href="#">Defining the Address Space and Specifying Address Resolution for MPLS VPNs over mGRE, page 14</a></li> </ul> <p>The following commands were introduced or modified by this feature: <b>set ip next-hop</b>, <b>show tunnel endpoints</b>, <b>tunnel mode</b>, <b>l3vpn encapsulation ip profile-name</b>, <b>protocol gre key</b>, <b>transport ipv4 source interface</b>.</p> |

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

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

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

© 2003—2009 Cisco Systems, Inc. All rights reserved.





## **MPLS Layer 3 VPNs: InterAutonomous Systems and Carrier Supporting Carrier**





# MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

---

**First Published: May 2, 2005**

**Last Updated: February 27, 2009**

The MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses feature allows a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) to span service providers and autonomous systems. This module explains how to enable Autonomous System Boundary Routers (ASBRs) to use Exterior Border Gateway Protocol (EBGP) to exchange IPv4 Network Layer Reachability Information (NLRI) in the form of VPN-IPv4 addresses.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses”](#) section on page 33.

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

## Contents

- [Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 2](#)
- [Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 3](#)
- [Information About MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 3](#)
- [How to Configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 11](#)
- [Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 16](#)



---

**Americas Headquarters:**

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

- [Command Reference, page 31](#)
- [Additional References, page 32](#)
- [Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 33](#)

## Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

- Before you configure EBGp routing between autonomous systems or subautonomous systems in an MPLS VPN, ensure that you have properly configured all MPLS VPN routing instances and sessions. The configuration tasks outlined in this section build from those configuration tasks. Perform the following tasks as described in the [Configuring MPLS Layer 3 VPNs](#) module:
  - Define VPN routing instances
  - Configure BGP routing sessions in the MPLS core
  - Configure PE-to-PE routing sessions in the MPLS core
  - Configure BGP PE-to-CE routing sessions
  - Configure a VPN-IPv4 EBGp session between directly connected ASBRs
- This feature is supported on the Cisco 12000 series router line cards listed in [Table 1](#).

**Table 1** Cisco 12000 Series Line Card Support Added for Cisco IOS Releases

| Type                    | Line Cards           | Cisco IOS Release Added |
|-------------------------|----------------------|-------------------------|
| Packet over SONET (POS) | 4-Port OC-3 POS      | 12.0(16)ST              |
|                         | 1-Port OC-12 POS     |                         |
|                         | 8-Port OC-3 POS      | 12.0(17)ST              |
|                         | 16-Port OC-3 POS     |                         |
|                         | 4-Port OC-12 POS     |                         |
|                         | 1-Port OC-48 POS     |                         |
|                         | 4-Port OC-3 POS ISE  | 12.0(22)S               |
|                         | 8-Port OC-3 POS ISE  |                         |
|                         | 16 x OC-3 POS ISE    |                         |
|                         | 4-Port OC-12 POS ISE |                         |
|                         | 1-Port OC-48 POS ISE |                         |
| Electrical interface    | 6-Port DS3           | 12.0(21)ST              |
|                         | 12-Port DS3          |                         |
|                         | 6-Port E3            | 12.0(22)S               |
|                         | 12-Port E3           |                         |
| Ethernet                | 3-Port GbE           | 12.0(23)S               |
|                         | 1-Port 10-GbE        | 12.0(24)S               |
|                         | Modular GbE/FE       |                         |
| ATM                     | 4-Port OC-3 ATM      | 12.0(16)ST              |
|                         | 1-Port OC-12 ATM     |                         |
|                         | 4-Port OC-12 ATM     | 12.0(17)ST              |
|                         | 8-Port OC-3 ATM      | 12.0(23)S               |

**Table 1** Cisco 12000 Series Line Card Support Added for Cisco IOS Releases

| Type                  | Line Cards                                                                                                                       | Cisco IOS Release Added |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Channelized interface | 2-Port CHOC-3<br>6-Port Ch T3 (DS1)<br>1-Port CHOC-12 (DS3)<br>1-Port CHOC-12 (OC-3)<br>4-Port CHOC-12 ISE<br>1-Port CHOC-48 ISE | 12.0(22)S               |

## Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Multihop VPN-IPv4 EBGp is not supported.

## Information About MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Before configuring this feature, you should understand the following concepts:

- [MPLS VPN Inter-AS Introduction, page 3](#)
- [Benefits of MPLS VPN Inter-AS, page 3](#)
- [Use of Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 4](#)
- [Information Exchange in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 4](#)

## MPLS VPN Inter-AS Introduction

An autonomous system is a single network or group of networks that is controlled by a common system administration group and that uses a single, clearly defined routing protocol.

As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. Also, some VPNs need to extend across multiple service providers (overlapping VPNs). Regardless of the complexity and location of the VPNs, the connection between autonomous systems must be seamless to the customer.

## Benefits of MPLS VPN Inter-AS

An MPLS VPN Inter-AS provides the following benefits:

- Allows a VPN to cross more than one service provider backbone

Service providers running separate autonomous systems can jointly offer MPLS VPN services to the same customer. A VPN can begin at one customer site and traverse different VPN service provider backbones before arriving at another site of the same customer. Previously, MPLS VPN could



traverses only a single BGP autonomous system service provider backbone. This feature allows multiple autonomous systems to form a continuous (and seamless) network between customer sites of a service provider.

- Allows a VPN to exist in different areas

A service provider can create a VPN in different geographic areas. Having all VPN traffic flow through one point (between the areas) allows for better rate control of network traffic between the areas.

- Allows confederations to optimize IBGP meshing

Internal Border Gateway Protocol (IBGP) meshing in an autonomous system is more organized and manageable. An autonomous system can be divided into multiple, separate subautonomous systems and then classify them into a single confederation (even though the entire VPN backbone appears as a single autonomous system). This capability allows a service provider to offer MPLS VPNs across the confederation because it supports the exchange of labeled VPN-IPv4 NLRI between the subautonomous systems that form the confederation.

## Use of Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Separate autonomous systems from different service providers can communicate by exchanging IPv4 NLRI in the form of VPN-IPv4 addresses. The ASBRs use EBGp to exchange that information. Then an Interior Gateway Protocol (IGP) distributes the network layer information for VPN-IPv4 prefixes throughout each VPN and each autonomous system. Routing information uses the following protocols:

- Within an autonomous system, routing information is shared using an IGP.
- Between autonomous systems, routing information is shared using an EBGp. An EBGp allows a service provider to set up an interdomain routing system that guarantees the loop-free exchange of routing information between separate autonomous systems.

The primary function of an EBGp is to exchange network reachability information between autonomous systems, including information about the list of autonomous system routes. The autonomous systems use EBGp border edge routers to distribute the routes, which include label switching information. Each border edge router rewrites the next hop and labels. See the [“Information Exchange in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses”](#) section for more information.

Interautonomous system configurations supported in an MPLS VPN are as follows:

- Interprovider VPN—MPLS VPNs that include two or more autonomous systems, connected by separate border edge routers. The autonomous systems exchange routes using EBGp. No IGP or routing information is exchanged between the autonomous systems.
- BGP confederations—MPLS VPNs that divide a single autonomous system into multiple subautonomous systems, and classify them as a single, designated confederation. The network recognizes the confederation as a single autonomous system. The peers in the different autonomous systems communicate over EBGp sessions; however, they can exchange route information as if they were IBGP peers.

## Information Exchange in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

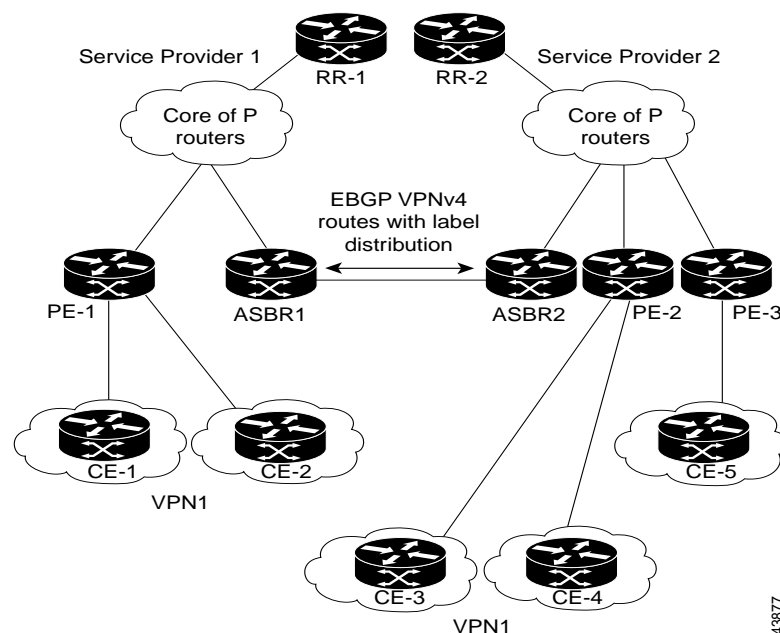
This section contains the following topics:

- [Transmission of Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 5](#)
- [Exchange of VPN Routing Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 6](#)
- [Packet Forwarding Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses, page 8](#)
- [Use of a Confederation for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 9](#)

## Transmission of Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Figure 1 illustrates one MPLS VPN consisting of two separate autonomous systems. Each autonomous system operates under different administrative control and runs a different IGP. Service providers exchange routing information through EBGP border edge routers (ASBR1, ASBR2).

**Figure 1** *EBGP Connection Between Two MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses*



This configuration uses the following process to transmit information:

- 
- Step 1** The provider edge router (PE-1) assigns a label for a route before distributing that route. The PE router uses the multiprotocol extensions of BGP to transmit label mapping information. The PE router distributes the route as a VPN-IPv4 address. The address label and the VPN identifier are encoded as part of the NLRI.
- Step 2** The two route reflectors (RR-1 and RR-2) reflect VPN-IPv4 internal routes within the autonomous system. The autonomous systems' border edge routers (ASBR1 and ASBR2) advertise the VPN-IPv4 external routes.

- Step 3** The EBGp border edge router (ASBR1) redistributes the route to the next autonomous system (ASBR2). ASBR1 specifies its own address as the value of the EBGp next-hop attribute and assigns a new label. The address ensures the following:
- That the next-hop router is always reachable in the service provider (P) backbone network.
  - That the label assigned by the distributing router is properly interpreted. (The label associated with a route must be assigned by the corresponding next-hop router.)
- Step 4** The EBGp border edge router (ASBR2) redistributes the route in one of the following ways, depending on its configuration:
- If the IBGP neighbors are configured with the **neighbor next-hop-self** command, ASBR2 changes the next-hop address of updates received from the EBGp peer, then forwards it.
  - If the IBGP neighbors are not configured with the **neighbor next-hop-self** command, the next-hop address does not get changed. ASBR2 must propagate a host route for the EBGp peer through the IGP. To propagate the EBGp VPN-IPv4 neighbor host route, use the **redistribute connected subnets** command. The EBGp VPN-IPv4 neighbor host route is automatically installed in the routing table when the neighbor comes up. This is essential to establish the label switched path between PE routers in different autonomous systems.
- 

## Exchange of VPN Routing Information in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Autonomous systems exchange VPN routing information (routes and labels) to establish connections. To control connections between autonomous systems, the PE routers and EBGp border edge routers maintain a Label Forwarding Information Base (LFIB). The LFIB manages the labels and routes that the PE routers and EBGp border edge routers receive during the exchange of VPN information.

Figure 2 illustrates the exchange of VPN route and label information between autonomous systems. The autonomous systems use the following conditions to exchange VPN routing information:

- Routing information includes:
  - The destination network (N)
  - The next-hop field associated with the distributing router
  - A local MPLS label (L)
- An RD1: route distinguisher is part of a destination network address. It makes the VPN-IPv4 route globally unique in the VPN service provider environment.
- The ASBRs are configured to change the next-hop (next hop-self) when sending VPN-IPv4 NLRI to the IBGP neighbors. Therefore, the ASBRs must allocate a new label when they forward the NLRI to the IBGP neighbors.

**Figure 2** *Exchanging Routes and Labels Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses*

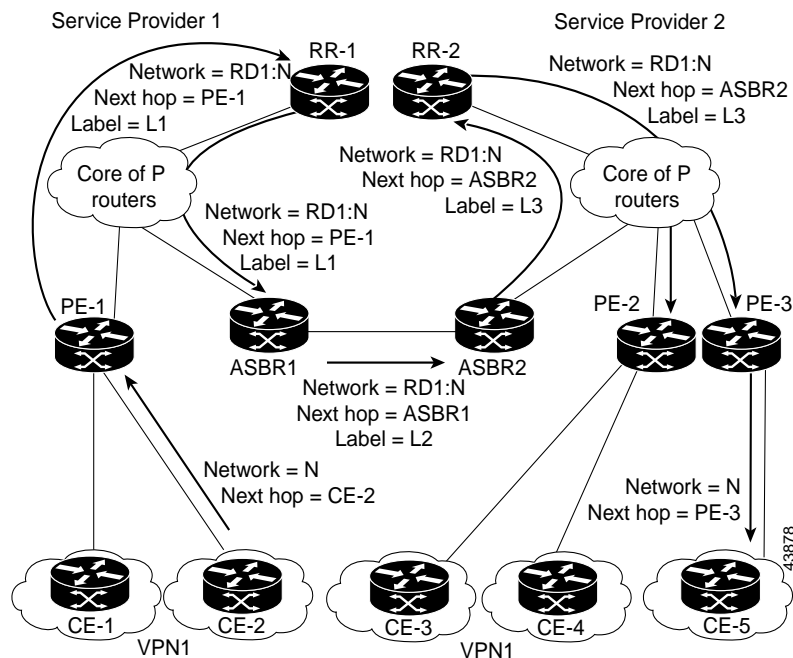
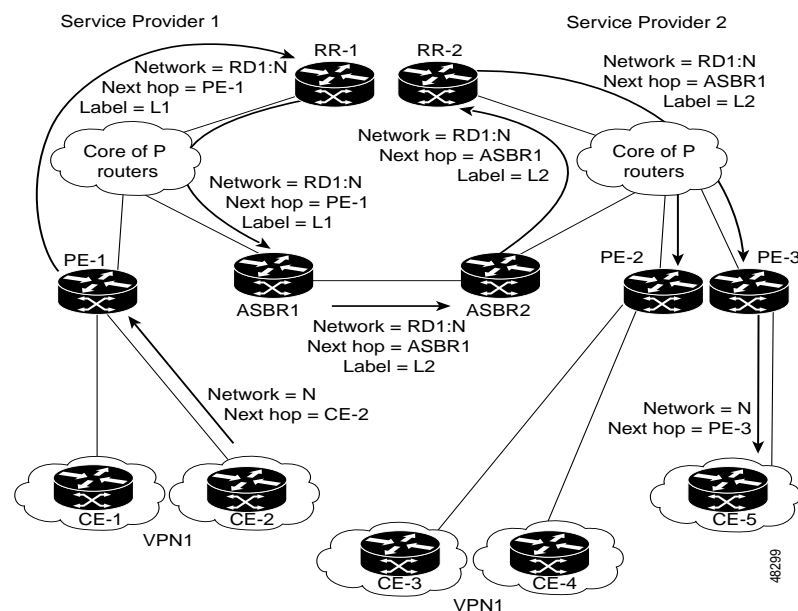


Figure 3 illustrates the exchange of VPN route and label information between autonomous systems. The only difference is that ASBR2 is configured with the **redistribute connected** command, which propagates the host routes to all PEs. The **redistribute connected** command is necessary because ASBR2 is not configured to change the next-hop address.

**Figure 3** *Exchanging Routes and Labels with the redistribute connected Command in an MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses*



## Packet Forwarding Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses

Figure 4 illustrates how packets are forwarded between autonomous systems in an interprovider network using the following packet forwarding method.

Packets are forwarded to their destination by means of MPLS. Packets use the routing information stored in the LFIB of each PE router and EBGP border edge router.

The service provider VPN backbone uses dynamic label switching to forward labels.

Each autonomous system uses standard multilevel labeling to forward packets between the edges of the autonomous system routers (for example, from CE-5 to PE-3). Between autonomous systems, only a single level of labeling is used, corresponding to the advertised route.

A data packet carries two levels of labels when traversing the VPN backbone:

- The first label (IGP route label) directs the packet to the correct PE router or EBGP border edge router. (For example, the IGP label of ASBR2 points to the ASBR2 border edge router.)
- The second label (VPN route label) directs the packet to the appropriate PE router or EBGP border edge router.

**Figure 4** Forwarding Packets Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses

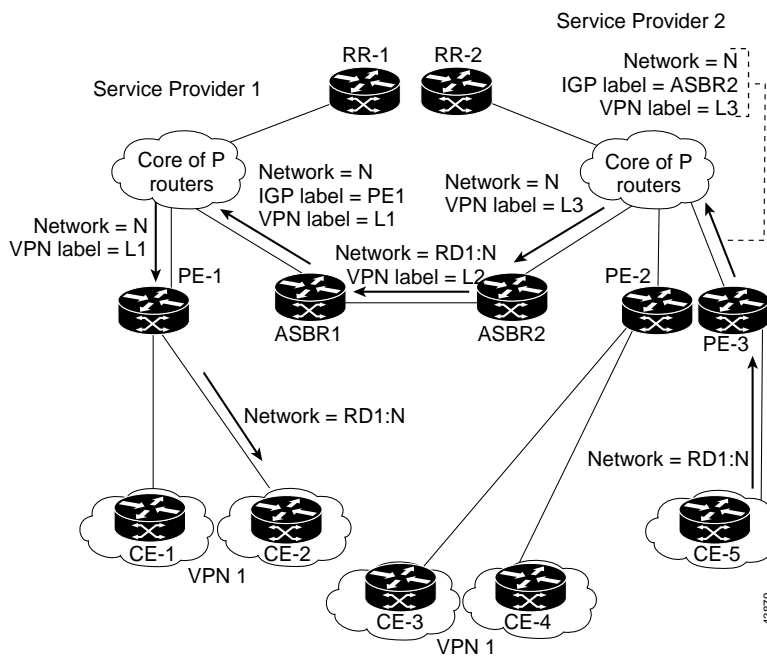
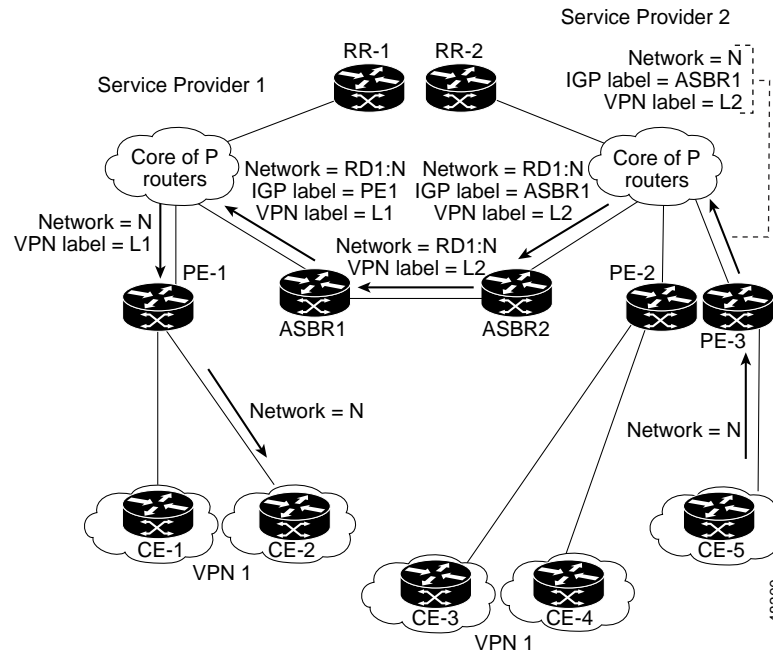


Figure 5 shows the same packet forwarding method as described in Figure 4, except the EBGp router (ASBR1) forwards the packet without reassigning it a new label.

**Figure 5 Forwarding Packets Without a New Label Assignment Between MPLS VPN Inter-AS Systems with ASBRs Exchanging VPN-IPv4 Addresses**



## Use of a Confederation for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

A confederation is multiple subautonomous systems grouped together. A confederation reduces the total number of peer devices in an autonomous system. A confederation divides an autonomous system into subautonomous systems and assigns a confederation identifier to the autonomous systems. A VPN can span service providers running in separate autonomous systems or in multiple subautonomous systems that form a confederation.

In a confederation, each subautonomous system is fully meshed with other subautonomous systems. The subautonomous systems communicate using an IGP, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). Each subautonomous system also has an EBGp connection to the other subautonomous systems. The confederation EBGp (CEBGp) border edge routers forward next-hop-self addresses between the specified subautonomous systems. The next-hop-self address forces the BGP to use a specified address as the next hop rather than letting the protocol choose the next hop.

You can configure a confederation with separate subautonomous systems in either of two ways:

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

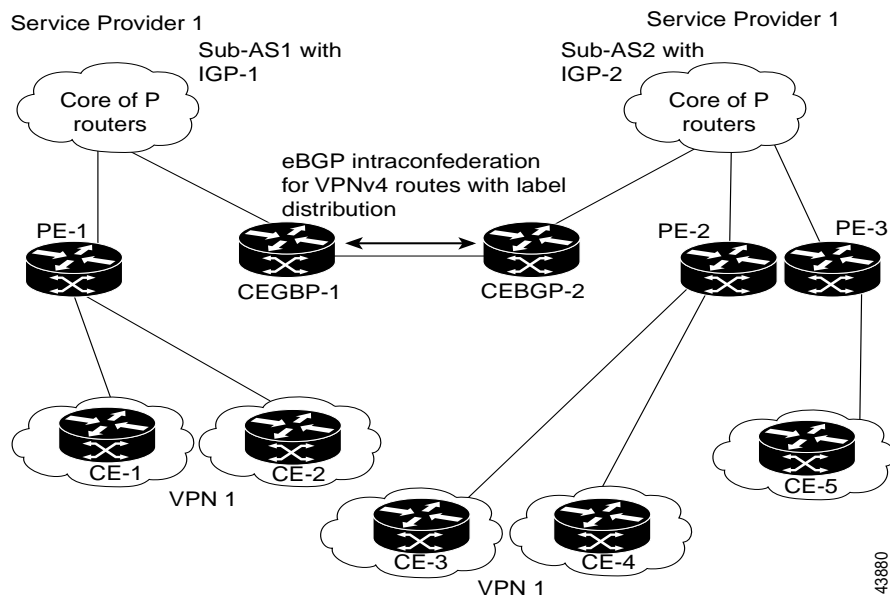
**Note**

Figure 2 and Figure 3 illustrate how two autonomous systems exchange routes and forward packets. Subautonomous systems in a confederation use a similar method of exchanging routes and forwarding packets.

Figure 6 illustrates a typical MPLS VPN confederation configuration. In this confederation configuration:

- The two CEBGP border edge routers exchange VPN-IPv4 addresses with labels between the two subautonomous systems.
- The distributing router changes the next-hop addresses and labels and uses a next-hop-self address.
- IGP-1 and IGP-2 know the addresses of CEBGP-1 and CEBGP-2.

**Figure 6** *EBGP Connection Between Two Subautonomous Systems in a Confederation*



In this confederation configuration:

- CEBGP border edge routers function as neighboring peers between the subautonomous systems. The subautonomous systems use EBGP to exchange route information.
- Each CEBGP border edge router (CEBGP-1, CEBGP-2) assigns a label for the route before distributing the route to the next subautonomous system. The CEBGP border edge router distributes the route as a VPN-IPv4 address by using the multiprotocol extensions of BGP. The label and the VPN identifier are encoded as part of the NLRI.
- Each PE and CEBGP border edge router assigns its own label to each VPN-IPv4 address prefix before redistributing the routes. The CEBGP border edge routers exchange VPN-IPv4 addresses with the labels. The next-hop-self address is included in the label (as the value of the EBGP next-hop attribute). Within the subautonomous systems, the CEBGP border edge router address is distributed throughout the IGP neighbors, and the two CEBGP border edge routers are known to both confederations.

# How to Configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

To configure MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, perform the tasks in the following sections:

- [Configuring the ASBRs to Exchange VPN-IPv4 Addresses, page 11](#) (required)
- [Configuring EBGp Routing to Exchange VPN Routes Between Subautonomous Systems in a Confederation, page 12](#) (required)
- [Verifying Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses, page 15](#) (optional)

## Configuring the ASBRs to Exchange VPN-IPv4 Addresses

To configure an EBGp ASBR to exchange VPN-IPv4 routes with another autonomous system, perform this task.



### Note

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default route-target filter**
5. **address-family vpnv4** [unicast]
6. **neighbor** *peer-group-name* **remote-as** *as-number*
7. **neighbor** *peer-group-name* **activate**
8. **exit-address-family**
9. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |



|               | Command or Action                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 1                                                    | Creates an EBGp routing process and assigns it an autonomous system number. <ul style="list-style-type: none"> <li>The autonomous system number is passed along and identifies the router to EBGp routers in another autonomous system.</li> </ul>                                                                                                     |
| <b>Step 4</b> | <b>no bgp default route-target filter</b><br><br><b>Example:</b><br>Router(config)# no bgp default route-target filter                       | Disables BGP route-target filtering and places the router in configuration mode. <ul style="list-style-type: none"> <li>All received BGP VPN-IPv4 routes are accepted by the router.</li> </ul>                                                                                                                                                        |
| <b>Step 5</b> | <b>address-family vpnv4 [<i>unicast</i>]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                           | Configures a routing session to carry VPNv4 addresses across the VPN backbone and places the router in address family configuration mode. <ul style="list-style-type: none"> <li>Each address has been made globally unique by the addition of an 8-byte route distinguisher (RD).</li> <li>The unicast keyword specifies a unicast prefix.</li> </ul> |
| <b>Step 6</b> | <b>neighbor <i>peer-group-name</i> remote-as <i>as-number</i></b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 1 remote-as 2 | Enters the address family configuration mode and specifies a neighboring EBGp peer group. <ul style="list-style-type: none"> <li>This EBGp peer group is identified to the specified autonomous system.</li> </ul>                                                                                                                                     |
| <b>Step 7</b> | <b>neighbor <i>peer-group-name</i> activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 1 activate                      | Activates the advertisement of the VPNv4 address family to a neighboring EBGp router.                                                                                                                                                                                                                                                                  |
| <b>Step 8</b> | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                           | Exits from the address family submode of the router configuration mode.                                                                                                                                                                                                                                                                                |
| <b>Step 9</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                     | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                         |

## Configuring EBGp Routing to Exchange VPN Routes Between Subautonomous Systems in a Confederation

Perform this task to configure EBGp routing to exchange VPN routes between subautonomous systems in a confederation.

**Note**

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

**Note**

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

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *sub-autonomous-system*
4. **bgp confederation identifier** *as-number*
5. **bgp confederation peers** *sub-autonomous-system*
6. **no bgp default route-target filter**
7. **address-family vpnv4 [unicast]**
8. **neighbor** *peer-group-name* **remote-as** *as-number*
9. **neighbor** *peer-group-name* **next-hop-self**
10. **neighbor** *peer-group-name* **activate**
11. **exit-address-family**
12. **end**

**DETAILED STEPS**

|        | Command or Action                               | Purpose                                                                                                                                                                  |
|--------|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                   | Enables privileged EXEC mode.                                                                                                                                            |
|        | <b>Example:</b><br>Router> enable               | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                       |
| Step 2 | <b>configure terminal</b>                       | Enters global configuration mode.                                                                                                                                        |
|        | <b>Example:</b><br>Router# configure terminal   |                                                                                                                                                                          |
| Step 3 | <b>router bgp</b> <i>sub-autonomous-system</i>  | Creates an EBGP routing process and assigns it an autonomous system number and enters the router in configuration mode.                                                  |
|        | <b>Example:</b><br>Router(config)# router bgp 2 | <ul style="list-style-type: none"> <li>The subautonomous system number is passed along to identify the router to EBGP routers in other subautonomous systems.</li> </ul> |

|         | Command or Action                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                 |
|---------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <b>bgp confederation identifier</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# bgp confederation identifier 100 | Defines an EBGp confederation by specifying a confederation identifier associated with each subautonomous system. <ul style="list-style-type: none"> <li>The subautonomous systems appear as a single autonomous system.</li> </ul>                                                                     |
| Step 5  | <b>bgp confederation peers</b> <i>sub-autonomous-system</i><br><br><b>Example:</b><br>Router(config-router)# bgp confederation peers 1 | Specifies the subautonomous systems that belong to the confederation (identifies neighbors of other subautonomous systems within the confederation as special EBGp peers).                                                                                                                              |
| Step 6  | <b>no bgp default route-target filter</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default route-target filter          | Disables BGP route-target community filtering. All received BGP VPN-IPv4 routes are accepted by the router.                                                                                                                                                                                             |
| Step 7  | <b>address-family vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                   | Configures a routing session to carry VPNv4 addresses across the VPN backbone. Each address is made globally unique by the addition of an 8-byte RD. Enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies a unicast prefix.</li> </ul> |
| Step 8  | <b>neighbor peer-group-name remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 1 remote-as 1  | Enters the address family configuration mode and specifies a neighboring EBGp peer group. <ul style="list-style-type: none"> <li>This EBGp peer group is identified to the specified subautonomous system.</li> </ul>                                                                                   |
| Step 9  | <b>neighbor peer-group-name next-hop-self</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 1 next-hop-self             | Advertises the router as the next hop for the specified neighbor. <ul style="list-style-type: none"> <li>If a next-hop-self address is specified as part of the router configuration, the <b>redistribute connected</b> command need not be used.</li> </ul>                                            |
| Step 10 | <b>neighbor peer-group-name activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor R activate                       | Activates the advertisement of the VPNv4 address family to a neighboring PE router in the specified subautonomous system.                                                                                                                                                                               |
| Step 11 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                     | Exits from the address family submode of the router configuration mode.                                                                                                                                                                                                                                 |
| Step 12 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                               | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                          |

## Verifying Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

Perform this task to display the VPN-IPv4 LFIB entries.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** {all | rd route-distinguisher | vrf vrf-name} [summary] [labels]
3. **show mpls forwarding-table** [network {mask | length} | labels label [-label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]
4. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                               |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                    |
| Step 2 | <b>show ip bgp vpnv4</b> {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]<br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all labels                                                                                   | Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>• Use the <b>all</b> and <b>labels</b> keywords to display information about all VPNv4 labels.</li> </ul> |
| Step 3 | <b>show mpls forwarding-table</b> [network {mask   length}   labels label [-label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]] [vrf vrf-name] [detail]<br><br><b>Example:</b><br>Router# show mpls forwarding-table | Displays the contents of the MPLS LFIB (such as VPNv4 prefix/length and BGP next-hop destination for the route).                                                                                      |
| Step 4 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                   | Exits to user EXEC mode.                                                                                                                                                                              |

### Examples

The sample output from the **show mpls forwarding-table** command shows how the VPN-IPv4 LFIB entries appear:

```
Router# show mpls forwarding-table
```

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

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

## Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

This section provides the following configuration examples for MPLS VPN Inter-AS:

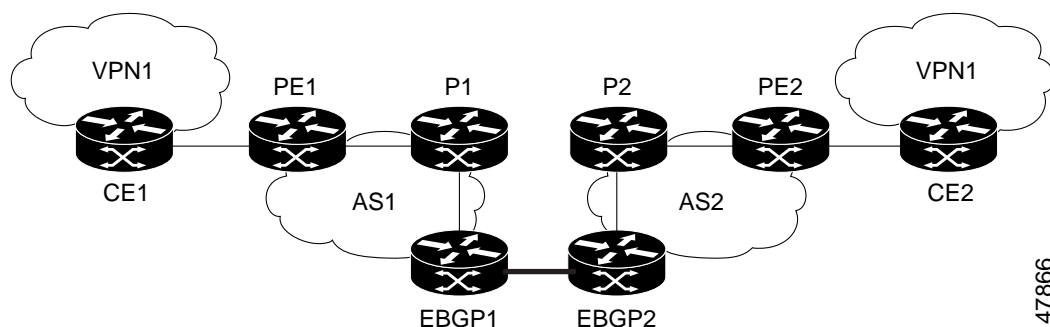
- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses: Example, page 16](#)
- [Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses in a Confederation: Example, page 23](#)

### Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses: Example

The network topology in [Figure 7](#) shows two autonomous systems, which are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, and EBG1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, and EBG2. The IGP is IS-IS.
- CE1 and CE2 belong to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- EBG1 is configured with the **redistribute connected subnets** command.
- EBG2 is configured with the **neighbor next-hop-self** command.

**Figure 7** Configuring Two Autonomous Systems



47866

### Configuration for Autonomous System 1, CE1: Example

The following example shows how to configure CE1 in VPN1 in a topology with two autonomous systems (see [Figure 7](#)):

```
CE1: Burlington
!
interface Loopback1
```

```

ip address aa.0.0.6 255.255.255.255
!
interface Serial1/3
description wychmere
no ip address
encapsulation frame-relay
frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
description wychmere
ip address aa.6.2.1 255.255.255.252
frame-relay interface-dlci 22
!
router ospf 1
network aa.0.0.0 0.255.255.255 area 0

```

## Configuration for Autonomous System 1, PE1: Example

The following example shows how to configure PE1 in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```

PE1: wychmere
!
ip cef
!
ip vrf V1
rd 1:105
route-target export 1:100
route-target import 1:100
!
interface Serial0/0
description Burlington
no ip address
encapsulation frame-relay
no fair-queue
clockrate 2000000
!
interface Serial0/0.3 point-to-point
description Burlington
ip vrf forwarding V1
ip address aa.6.2.2 255.255.255.252
frame-relay interface-dlci 22
!
interface Ethernet0/1
description Vermont
ip address aa.2.2.5 255.255.255.0
tag-switching ip
!
router ospf 1
log-adjacency-changes
network aa.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
log-adjacency-changes
redistribute bgp 1 metric 100 subnets
network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
no synchronization
neighbor 1 peer-group
neighbor 1 remote-as 1
neighbor 1 update-source Loopback0

```

```

neighbor aa.0.0.2 peer-group R
no auto-summary
!
address-family ipv4 vrf V1
 redistribute ospf 10
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 exit-address-family

```

## Configuration for Autonomous System 1, P1: Example

The following example shows how to configure P1 in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```

P1: Vermont
!
ip cef
!
interface Loopback0
 ip address aa.0.0.2 255.255.255.255
!
interface Ethernet0/1
 description Ogunquit
 ip address aa.2.1.1 255.255.255.0
 tag-switching ip
!
interface FastEthernet2/0
 description wychmere
 ip address aa.2.2.1 255.255.255.0
 duplex auto
 speed auto
 tag-switching ip
!
router ospf 1
 log-adjacency-changes
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor aa.0.0.4 peer-group R
 neighbor aa.0.0.5 peer-group R
!
address-family vpnv4
 neighbor R activate
 neighbor R route-reflector-client
 neighbor R send-community extended
 neighbor aa.0.0.4 peer-group R
 neighbor aa.0.0.5 peer-group R
 exit-address-family

```

## Configuration for Autonomous System 1, EBG1: Example

The following example shows how to configure EBG1 in AS1 in a topology with two autonomous systems (see [Figure 7](#)):

```
EBG1: Ogunquit
!
ip cef
!
interface Loopback0
 ip address aa.0.0.4 255.255.255.255
!
EBG1: Ogunquit
!
ip cef
!
interface Loopback0
 ip address aa.0.0.4 255.255.255.255
!
interface Ethernet0/1
 description Vermont
 ip address aa.2.1.40 255.255.255.0
 tag-switching ip
!
interface ATM1/0
 description Lowell
 no ip address
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 description Lowell
 ip address aa.0.0.1 255.255.255.252
 pvc 1/100
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor aa.0.0.2 remote-as 2
 neighbor aa.0.0.2 peer-group R
 no auto-summary
!
address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 activate
 neighbor aa.0.0.2 send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
 exit-address-family
```



## Configuration for Autonomous System 2, EBG2: Example

The following example shows how to configure EBG2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```
EBGP2: Lowell
!
ip cef
!
ip vrf V1
  rd 2:103
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address aa.0.0.3 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address aa.0.0.3 255.255.255.255
!
interface Serial0/0
  description Littleton
  no ip address
  encapsulation frame-relay
  load-interval 30
  no fair-queue
  clockrate 2000000
!
interface Serial0/0.2 point-to-point
  description Littleton
  ip unnumbered Loopback0
  ip router isis
  tag-switching ip
  frame-relay interface-dlci 23
!
interface ATM1/0
  description Ogunquit
  no ip address
  atm clock INTERNAL
  no atm scrambling cell-payload
  no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
  description Ogunquit
  ip address aa.0.0.2 255.255.255.252
  pvc 1/100
!
router isis
  net 49.0002.0000.0000.0003.00
!
router bgp 2
  no synchronization
  no bgp default route-target filter
  bgp log-neighbor-changes
  neighbor aa.0.0.1 remote-as 1
  neighbor aa.0.0.8 remote-as 2
  neighbor aa.0.0.8 update-source Loopback0
  neighbor aa.0.0.8 next-hop-self
!
address-family ipv4 vrf V1
  redistribute connected
```

```

no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor aa.0.0.1 activate
neighbor aa.0.0.1 send-community extended
neighbor aa.0.0.8 activate
neighbor aa.0.0.8 next-hop-self
neighbor aa.0.0.8 send-community extended
exit-address-family

```

## Configuration for Autonomous System 2, P2: Example

The following example shows how to configure P2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```

P2: Littleton
!
ip cef
!
ip vrf V1
rd 2:108
route-target export 1:100
route-target import 1:100
!
interface Loopback0
ip address aa.0.0.8 255.255.255.255
ip router isis
!
interface Loopback1
ip vrf forwarding V1
ip address aa.0.0.8 255.255.255.255
!
interface FastEthernet0/0
description Pax
ip address aa.9.1.2 255.255.255.0
ip router isis
tag-switching ip
!
interface Serial5/0
description Lowell
no ip address
encapsulation frame-relay
frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
description Lowell
ip unnumbered Loopback0
ip router isis
tag-switching ip
frame-relay interface-dlci 23
!
router isis
net aa.0002.0000.0000.0008.00
!
router bgp 2
no synchronization
bgp log-neighbor-changes
neighbor R peer-group
neighbor R remote-as 2
neighbor R update-source Loopback0

```

```

neighbor R route-reflector-client
neighbor aa.0.0.3 peer-group R
neighbor aa.0.0.9 peer-group R
!
address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor aa.0.0.3 peer-group R
  neighbor aa.0.0.9 peer-group R
  exit-address-family

```

## Configuration for Autonomous System 2, PE2: Example

The following example shows how to configure PE2 in AS2 in a topology with two autonomous systems (see [Figure 7](#)):

```

PE2: Pax
!
ip cef
!
ip vrf V1
  rd 2:109
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address aa.0.0.9 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address aa.0.0.9 255.255.255.255
!
interface Serial0/0
  description Bethel
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  no fair-queue
  clockrate 2000000
!
interface Serial0/0.1 point-to-point
  description Bethel
  ip vrf forwarding V1
  ip unnumbered Loopback1
  frame-relay interface-dlci 24
!
interface FastEthernet0/1
  description Littleton
  ip address aa.9.1.1 255.255.255.0
  ip router isis
  tag-switching ip
!
router ospf 10 vrf V1
  log-adjacency-changes

```

```

redistribute bgp 2 subnets
network aa.0.0.0 0.255.255.255 area 0
!
router isis
net 49.0002.0000.0000.0009.00
!
router bgp 2
no synchronization
bgp log-neighbor-changes
neighbor aa.0.0.8 remote-as 2
neighbor aa.0.0.8 update-source Loopback0
!
address-family ipv4 vrf V1
redistribute connected
redistribute ospf 10
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor aa.0.0.8 activate
neighbor aa.0.0.8 send-community extended
exit-address-family v

```

## Configuration for Autonomous System 2, CE2: Example

The following example shows how to configure CE2 in VPN1 in a topology with two autonomous systems (see [Figure 7](#)):

```

CE2: Bethel
!
interface Loopback0
ip address 1.0.0.11 255.255.255.255
!
interface Serial0
description Pax
no ip address
encapsulation frame-relay
no fair-queue
clockrate 2000000
!
interface Serial0.1 point-to-point
description Pax
ip unnumbered Loopback0
frame-relay interface-dlci 24
!
router ospf 1
network aa.0.0.0 0.255.255.255 area 0

```

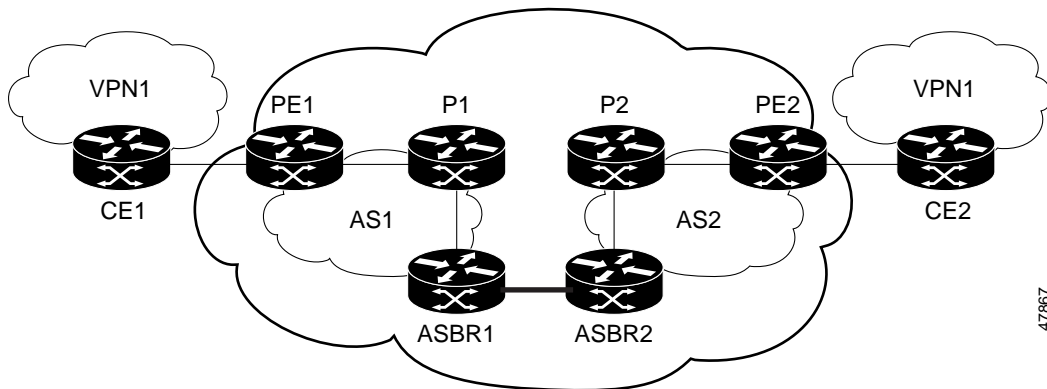
## Configuring MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses in a Confederation: Example

The network topology in [Figure 8](#) shows a single internet service provider, which is partitioning the backbone with confederations. The autonomous system number of the provider is 100. The two autonomous systems run their own IGP and are configured as follows:

- Autonomous system 1 (AS1) includes PE1, P1, CEBGP1. The IGP is OSPF.
- Autonomous system 2 (AS2) includes PE2, P2, CEBGP2. The IGP is IS-IS.

- CE1 and CE2 belong to the same VPN, which is called VPN1.
- The P routers are route reflectors.
- CEBGP1 is configured with the **redistribute connected subnets** command.
- CEBGP2 is configured with the **neighbor next-hop-self** command.

**Figure 8** *Configuring Two Autonomous Systems in a Confederation*



## Configuration for Autonomous System 1, CE1: Example

The following example shows how to configure CE1 in VPN1 in a confederation topology (see [Figure 8](#)):

```
CE1: Burlington
!
interface Loopback1
 ip address aa.0.0.6 255.255.255.255
!
interface Serial1/3
 description wychmere
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial1/3.1 point-to-point
 description wychmere
 ip address aa.6.2.1 255.255.255.252
 frame-relay interface-dlci 22
!
router ospf 1
 network aa.0.0.0 0.255.255.255 area 0
```

## Configuration for Autonomous System 1, PE1: Example

The following example shows how to configure PE1 in AS1 in a confederation topology (see [Figure 8](#)):

```
PE1: wychmere
!
ip cef
!
ip vrf V1
 rd 1:105
 route-target export 1:100
```

```

route-target import 1:100
!
interface Serial0/0
description Burlington
no ip address
encapsulation frame-relay
no fair-queue
clockrate 2000000
!
interface Serial0/0.3 point-to-point
description Burlington
ip vrf forwarding V1
ip address aa.6.2.2 255.255.255.252
frame-relay interface-dlci 22
!
interface Ethernet0/1
description Vermont
ip address aa.2.2.5 255.255.255.0
tag-switching ip
!
router ospf 1
log-adjacency-changes
network aa.0.0.0 0.255.255.255 area 0
!
router ospf 10 vrf V1
log-adjacency-changes
redistribute bgp 1 metric 100 subnets
network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
no synchronization
bgp confederation identifier 100
bgp confederation identifier 100
neighbor 1 peer-group
neighbor 1 remote-as 1
neighbor 1 update-source Loopback0
neighbor aa.0.0.2 peer-group R
no auto-summary
!
address-family ipv4 vrf V1
redistribute ospf 10
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor R activate
neighbor R send-community extended
neighbor aa.0.0.2 peer-group R
no auto-summary
exit-address-family

```

## Configuration for Autonomous System 1, P1 Example

The following example shows how to configure P1 in AS1 in a confederation topology (see [Figure 8](#)):

```

P1: Vermont
!
ip cef
!
interface Loopback0
ip address aa.0.0.2 255.255.255.255

```

```

!
interface Ethernet0/1
  description Ogunquit
  ip address 100.2.1.1 255.255.255.0
  tag-switching ip
!
interface FastEthernet2/0
  description wychmere
  ip address aa.2.2.1 255.255.255.0
  duplex auto
  speed auto
  tag-switching ip
!
router ospf 1
  log-adjacency-changes
  network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
  no synchronization
  bgp log-neighbor-changes
  bgp confederation identifier 100
  neighbor R peer-group
  neighbor R remote-as 1
  neighbor R update-source Loopback0
  neighbor R route-reflector-client
  neighbor 100.0.0.4 peer-group R
  neighbor 100.0.0.5 peer-group R
!
address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor aa.0.0.4 peer-group R
  neighbor aa.0.0.5 peer-group R
  exit-address-family

```

## Configuration for Autonomous System 1, CEBGP1: Example

The following example shows how to configure CEBGP1 in AS1 in a confederation topology (see [Figure 8](#)):

```

EBGP1: Ogunquit
!
ip cef
!
interface Loopback0
  ip address aa.0.0.4 255.255.255.255
!
interface Ethernet0/1
  description Vermont
  ip address aa.2.1.40 255.255.255.0
  tag-switching ip
!
interface ATM1/0
  description Lowell
  no ip address
  no atm scrambling cell-payload
  no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
  description Lowell

```

```

ip address aa.0.0.1 255.255.255.252
pvc 1/100
!
router ospf 1
 log-adjacency-changes
 redistribute connected subnets
 network aa.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp confederation identifier 100
 bgp confederation peers 1
 neighbor R peer-group
 neighbor R remote-as 1
 neighbor R update-source Loopback0
 neighbor aa.0.0.2 remote-as 2
 neighbor aa.0.0.2 next-hop-self
 neighbor aa.0.0.2 peer-group R
 no auto-summary
!
address-family vpnv4
 neighbor R activate
 neighbor R send-community extended
 neighbor aa.0.0.2 activate
 neighbor aa.0.0.2 next-hop-self
 neighbor aa.0.0.2 send-community extended
 neighbor aa.0.0.2 peer-group R
 no auto-summary
exit-address-family

```

## Configuration for Autonomous System 2, CEBGP2: Example

The following example shows how to configure CEBGP2 in AS2 in a confederation topology (see [Figure 8](#)):

```

EBGP2: Lowell
!
ip cef
!
ip vrf V1
 rd 2:103
 route-target export 1:100
 route-target import 1:100
!
interface Loopback0
 ip address aa.0.0.3 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.3 255.255.255.255
!
interface Serial0/0
 description Littleton
 no ip address
 encapsulation frame-relay
 load-interval 30
 no fair-queue
 clockrate 2000000

```



```

!
interface Serial0/0.2 point-to-point
description Littleton
ip unnumbered Loopback0
ip router isis
tag-switching ip
frame-relay interface-dlci 23
!
interface ATM1/0
description Ogunquit
no ip address
atm clock INTERNAL
no atm scrambling cell-payload
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
description Ogunquit
ip address aa.0.0.2 255.255.255.252
pvc 1/100
!
router isis
net aa.0002.0000.0000.0003.00
!
router bgp 2
no synchronization
no bgp default route-target filter
bgp log-neighbor-changes
bgp confederation identifier 100
bgp confederation peers 1
neighbor aa.0.0.1 remote-as 1
neighbor aa.0.0.1 next-hop-self
neighbor aa.0.0.8 remote-as 2
neighbor aa.0.0.8 update-source Loopback0
neighbor aa.0.0.8 next-hop-self
!
address-family ipv4 vrf V1
redistribute connected
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor aa.0.0.1 activate
neighbor aa.0.0.1 next-hop-self
neighbor aa.0.0.1 send-community extended
neighbor aa.0.0.8 activate
neighbor aa.0.0.8 next-hop-self
neighbor aa.0.0.8 send-community extended
exit-address-family

```

## Configuration for Autonomous System 2, P2: Example

The following example shows how to configure P2 in AS2 in a confederation topology (see [Figure 8](#)):

```

P2: Littleton
!
ip cef
!
ip vrf V1
rd 2:108
route-target export 1:100
route-target import 1:100

```

```

!
interface Loopback0
 ip address aa.0.0.8 255.255.255.255
 ip router isis
!
interface Loopback1
 ip vrf forwarding V1
 ip address aa.0.0.8 255.255.255.255
!
interface FastEthernet0/0
 description Pax
 ip address aa.9.1.2 255.255.255.0
 ip router isis
 tag-switching ip
!
interface Serial5/0
 description Lowell
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
!
interface Serial5/0.1 point-to-point
 description Lowell
 ip unnumbered Loopback0
 ip router isis
 tag-switching ip
 frame-relay interface-dlci 23
!
router isis
 net aa.0002.0000.0000.0008.00
!
router bgp 2
 no synchronization
 bgp log-neighbor-changes
 bgp confederation identifier 100
 neighbor R peer-group
 neighbor R remote-as 2
 neighbor R update-source Loopback0
 neighbor R route-reflector-client
 neighbor aa.0.0.3 peer-group R
 neighbor aa.0.0.9 peer-group R
!
 address-family ipv4 vrf V1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
 address-family vpnv4
  neighbor R activate
  neighbor R route-reflector-client
  neighbor R send-community extended
  neighbor aa.0.0.3 peer-group R
  neighbor aa.0.0.9 peer-group R
  exit-address-family

```

## Configuration for Autonomous System 2, PE2: Example

The following example shows how to configure PE2 in AS2 in a confederation topology (see [Figure 8](#)):

```

PE2: Pax
!

```

```

ip cef
!
ip vrf V1
  rd 2:109
  route-target export 1:100
  route-target import 1:100
!
interface Loopback0
  ip address aa.0.0.9 255.255.255.255
  ip router isis
!
interface Loopback1
  ip vrf forwarding V1
  ip address 1.0.0.9 255.255.255.255
!
interface Serial0/0
  description Bethel
  no ip address
  encapsulation frame-relay
  frame-relay intf-type dce
  no fair-queue
  clockrate 2000000
!
interface Serial0/0.1 point-to-point
  description Bethel
  ip vrf forwarding V1
  ip unnumbered Loopback1
  frame-relay interface-dlci 24
!
interface FastEthernet0/1
  description Littleton
  ip address 200.9.1.1 255.255.255.0
  ip router isis
  tag-switching ip
!
router ospf 10 vrf V1
  log-adjacency-changes
  redistribute bgp 2 subnets
  network aa.0.0.0 0.255.255.255 area 0
!
router isis
  net aa.0002.0000.0000.0009.00
!
router bgp 2
  no synchronization
  bgp log-neighbor-changes
  bgp confederation identifier 100
  neighbor aa.0.0.8 remote-as 2
  neighbor aa.0.0.8 update-source Loopback0
!
address-family ipv4 vrf V1
  redistribute connected
  redistribute ospf 10
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor aa.0.0.8 activate
  neighbor aa.0.0.8 send-community extended
  exit-address-family

```

## Configuration for Autonomous System 2, CE2: Example

The following example shows how to configure CE2 in VPN1 in a confederation topology (see [Figure 8](#)):

```
CE2: Bethel
!
interface Loopback0
 ip address aa.0.0.11 255.255.255.255
!
interface Serial0
 description Pax
 no ip address
 encapsulation frame-relay
 no fair-queue
 clockrate 2000000
!
interface Serial0.1 point-to-point
 description Pax
 ip unnumbered Loopback0
 frame-relay interface-dlci 24
!
router ospf 1
 network aa.0.0.0 0.255.255.255 area 0
```

## Command Reference

This feature uses no new or modified commands.

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

### MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

### RFCs

| RFC      | Title                                                         |
|----------|---------------------------------------------------------------|
| RFC 1700 | <i>Assigned Numbers</i>                                       |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i> |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                  |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                     |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                    |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

[Table 2](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

[Table 2](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

| Feature Name                            | Releases                                          | Feature Information                                                                                                                                                                                                                                   |
|-----------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Interautonomous System Support | 12.1(5)T<br>12.0(16)ST<br>12.0(17)ST<br>12.0(22)S | <p>This feature enables an MPLS VPN to span service providers and autonomous systems. This feature explains how to configuring the Inter-AS using the ASBRs to exchange VPN-IPv4 Addresses.</p> <p>This feature uses no new or modified commands.</p> |

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2005-2009 Cisco Systems, Inc. All rights reserved.



# MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

---

**First Published: May 2, 2005**

**Last Updated: February 27, 2009**

The MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels feature allows a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) to span service providers and autonomous systems. This module explains how to configure an MPLS VPN Inter-AS network so that the Autonomous System Boundary Routers (ASBRs) exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol, external Border Gateway Protocol (eBGP).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels” section on page 37](#).

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

## Contents

- [Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 2](#)
- [Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 3](#)



---

**Americas Headquarters:**

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



- [Information About MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 3](#)
- [How to Configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 6](#)
- [Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 20](#)
- [Command Reference, page 35](#)
- [Additional References, page 36](#)
- [Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 37](#)

## Prerequisites for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

The network must be properly configured for MPLS VPN operation before you configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels.

[Table 1](#) lists the Cisco 12000 series line card support in Cisco IOS S releases.

**Table 1** *Cisco 12000 Series Line Card Support in Cisco IOS S Releases*

| Type                  | Line Cards                                                                                                                       | Cisco IOS Release Supported        |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| ATM                   | 4-Port OC-3 ATM<br>1-Port OC-12 ATM<br>4-Port OC-12 ATM<br>8-Port OC-3 ATM                                                       | 12.0(22)S, 12.0(23)S,<br>12.0(27)S |
| Channelized interface | 2-Port CHOC-3<br>6-Port Ch T3 (DS1)<br>1-Port CHOC-12 (DS3)<br>1-Port CHOC-12 (OC-3)<br>4-Port CHOC-12 ISE<br>1-Port CHOC-48 ISE | 12.0(22)S, 12.0(23)S,<br>12.0(27)S |
| Electrical interface  | 6-Port DS3<br>12-Port DS3<br>6-Port E3<br>12-Port E3                                                                             | 12.0(22)S, 12.0(23)S,<br>12.0(27)S |
| Ethernet              | 3-Port GbE                                                                                                                       | 12.0(23)S, 12.0(27)S               |

**Table 1** Cisco 12000 Series Line Card Support in Cisco IOS S Releases (continued)

| Type                    | Line Cards                                                                                                                                                                                                                               | Cisco IOS Release Supported        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|
| Packet over SONET (POS) | 4-Port OC-3 POS<br>8-Port OC-3 POS<br>16-Port OC-3 POS<br>1-Port OC-12 POS<br>4-Port OC-12 POS<br>1-Port OC-48 POS<br>4-Port OC-3 POS ISE<br>8-Port OC-3 POS ISE<br>16-Port OC-3 POS ISE<br>4-Port OC-12 POS ISE<br>1-Port OC-48 POS ISE | 12.0(22)S, 12.0(23)S,<br>12.0(27)S |

## Restrictions for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

This feature includes the following restrictions:

- For networks configured with eBGP multihop, you must configure a label switched path (LSP) between nonadjacent routers.
- The physical interfaces that connect the BGP speakers must support Cisco Express Forwarding or distributed Cisco Express Forwarding and MPLS.

## Information About MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Before configuring MPLS VPN Inter-AS, you should understand the following concepts:

- [MPLS VPN Inter-AS Introduction, page 3](#)
- [Benefits of MPLS VPN Inter-AS, page 4](#)
- [Information About Using MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 4](#)
- [Benefits of MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels, page 4](#)
- [How the Inter-AS Works When ASBRs Exchange IPv4 Routes with MPLS Labels, page 5](#)

## MPLS VPN Inter-AS Introduction

An autonomous system is a single network or group of networks that is controlled by a common system administration group and that uses a single, clearly defined routing protocol.

As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. Also, some VPNs need to extend across multiple service providers (overlapping VPNs). Regardless of the complexity and location of the VPNs, the connection between autonomous systems must be seamless to the customer.

## Benefits of MPLS VPN Inter-AS

MPLS VPN Inter-AS provides the following benefits:

- Allows a VPN to cross more than one service provider backbone

Service providers running separate autonomous systems, can jointly offer MPLS VPN services to the same customer. A VPN can begin at one site and traverse different VPN service provider backbones before arriving at another site of the same customer. Previously, MPLS VPNs could traverse only a single BGP autonomous system service provider backbone. This feature allows multiple autonomous systems to form a continuous (and seamless) network between customer sites of a service provider.

- Allows a VPN to exist in different areas

A service provider can create a VPN in different geographic areas. Having all VPN traffic flow through one point (between the areas) allows for better rate control of network traffic between the areas.

- Allows confederations to optimize iBGP meshing

Internal Border Gateway Protocol (iBGP) meshing in an autonomous system is more organized and manageable. This feature can divide an autonomous system into multiple, separate subautonomous systems and then classify them into a single confederation (even though the entire VPN backbone appears as a single autonomous system). This capability allows a service provider to offer MPLS VPNs across the confederation because it supports the exchange of labeled VPN-IPv4 Network Layer Reachability Information (NLRI) between the subautonomous systems that form the confederation.

## Information About Using MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

This feature can configure a MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. RRs exchange VPN-IPv4 routes by using multihop, multiprotocol, External Border Gateway Protocol (eBGP). This method of configuring the Inter-AS system is often called MPLS VPN Inter-AS—IPv4 BGP Label Distribution.

## Benefits of MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

An Inter-AS system can be configured so that the ASBRs exchange the IPv4 routes and MPLS labels has the following benefits:

- Saves the ASBRs from having to store all the VPN-IPv4 routes. Using the route reflectors to store the VPN-IPv4 routes and forward them to the PE routers results in improved scalability compared with configurations where the ASBR holds all of the VPN-IPv4 routes and forwards the routes based on VPN-IPv4 labels.
- Simplifies the configuration at the border of the network by having the route reflectors hold the VPN-IPv4 routes.
- Enables a non-VPN core network to act as a transit network for VPN traffic. You can transport IPv4 routes with MPLS labels over a non-MPLS VPN service provider.

- Eliminates the need for any other label distribution protocol between adjacent LSRs. If two adjacent label switch routers (LSRs) are also BGP peers, BGP can handle the distribution of the MPLS labels. No other label distribution protocol is needed between the two LSRs.

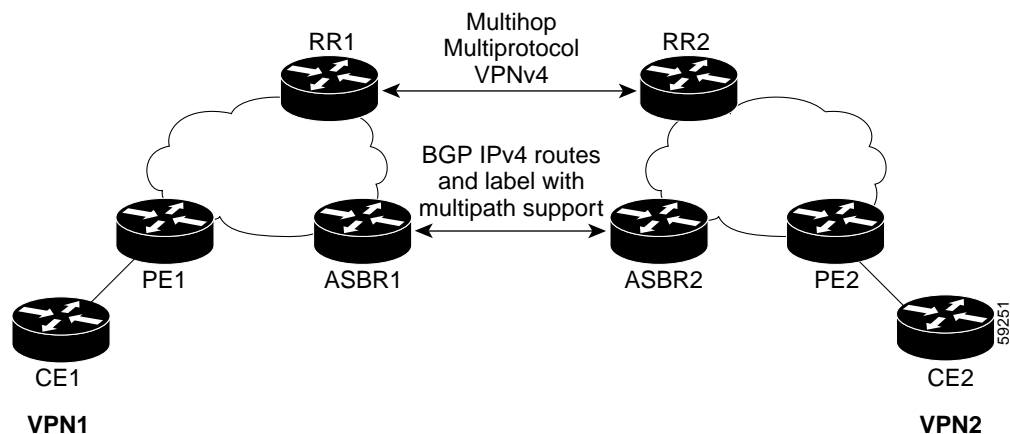
## How the Inter-AS Works When ASBRs Exchange IPv4 Routes with MPLS Labels

A VPN service provider network to exchange IPv4 routes with MPLS labels can be configured. The VPN service provider network can be configured as follows:

- Route reflectors exchange VPN-IPv4 routes by using multihop, multiprotocol eBGP. This configuration also preserves the next-hop information and the VPN labels across the autonomous systems.
- A local PE router (for example, PE1 in [Figure 1](#)) needs to know the routes and label information for the remote PE router (PE2). This information can be exchanged between the PE routers and ASBRs in one of two ways:
  - Internal Gateway Protocol (IGP) and Label Distribution Protocol (LDP): The ASBR can redistribute the IPv4 routes and MPLS labels it learned from eBGP into IGP and LDP and vice versa.
  - Internal Border Gateway Protocol (iBGP) IPv4 label distribution: The ASBR and PE router can use direct iBGP sessions to exchange VPN-IPv4 and IPv4 routes and MPLS labels.

Alternatively, the route reflector can reflect the IPv4 routes and MPLS labels learned from the ASBR to the PE routers in the VPN. This is accomplished by the ASBR exchanging IPv4 routes and MPLS labels with the route reflector. The route reflector also reflects the VPN-IPv4 routes to the PE routers in the VPN. For example, in VPN1 of [Figure 1](#), RR1 reflects to PE1 the VPN-IPv4 routes it learned and IPv4 routes and MPLS labels learned from ASBR1. Using the route reflectors to store the VPN-IPv4 routes and forward them through the PE routers and ASBRs allows for a scalable configuration.

**Figure 1** *VPNs Using eBGP and iBGP to Distribute Routes and MPLS Labels*



## BGP Routing Information

BGP routing information includes the following items:

- A network number (prefix), which is the IP address of the destination.
- Autonomous system path, which is a list of the other autonomous systems through which a route passes on its way to the local router. The first autonomous system in the list is closest to the local router; the last autonomous system in the list is farthest from the local router and usually the autonomous system where the route began.
- Path attributes, which provide other information about the autonomous system path, for example, the next hop.

## Types of BGP Messages and MPLS Labels

MPLS labels are included in the update messages that a router sends. Routers exchange the following types of BGP messages:

- Keepalive messages—Routers exchange keepalive messages to determine if a neighboring router is still available to exchange routing information. The router sends these messages at regular intervals. (Sixty seconds is the default for Cisco routers.) The keepalive message does not contain routing data; it contains only a message header.
- Notification messages—When a router detects an error, it sends a notification message.
- Open messages—After a router establishes a TCP connection with a neighboring router, the routers exchange open messages. This message contains the number of the autonomous system to which the router belongs and the IP address of the router that sent the message.
- Update messages—When a router has a new, changed, or broken route, it sends an update message to the neighboring router. This message contains the NLRI, which lists the IP addresses of the usable routes. The update message includes any routes that are no longer usable. The update message also includes path attributes and the lengths of both the usable and unusable paths. Labels for VPN-IPv4 routes are encoded in the update message as specified in RFC 2858. The labels for the IPv4 routes are encoded in the update message as specified in RFC 3107.

## How BGP Sends MPLS Labels with Routes

When BGP (eBGP and iBGP) distributes a route, it can also distribute an MPLS label that is mapped to that route. The MPLS label mapping information for the route is carried in the BGP update message that contains the information about the route. If the next hop is not changed, the label is preserved.

When you issue the **neighbor send-label** command on both BGP routers, the routers advertise to each other that they can then send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all outgoing BGP updates.

# How to Configure MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

To configure MPLS VPN Inter-AS with ASBRs exchanging IPv4 routes and MPLS labels, perform the tasks in the following sections:

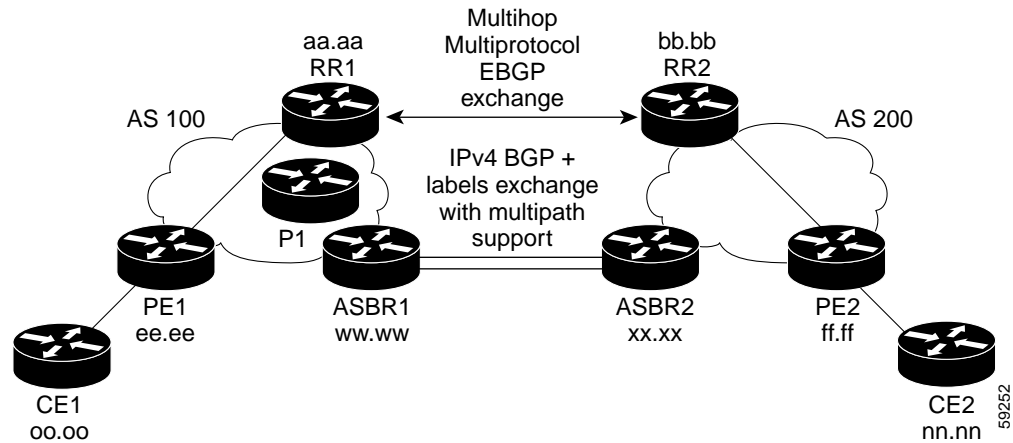
- [Configuring the ASBRs to Exchange IPv4 Routes and MPLS Labels, page 7](#)
- [Configuring the Route Reflectors to Exchange VPN-IPv4 Routes, page 9](#)
- [Configuring the Route Reflector to Reflect Remote Routes in Its Autonomous System, page 11](#)

- [Verifying the MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels Configuration, page 13](#)

Figure 2 shows the following sample configuration:

- The configuration consists of two VPNs.
- The ASBRs exchange the IPv4 routes with MPLS labels.
- The route reflectors exchange the VPN-IPv4 routes using multihop MPLS eBGP.
- The route reflectors reflect the IPv4 and VPN-IPv4 routes to the other routers in their autonomous system.

**Figure 2** *Configuring Two VPN Service Providers to Exchange IPv4 Routes and MPLS Labels*



## Configuring the ASBRs to Exchange IPv4 Routes and MPLS Labels

Perform this task to configure the ASBRs to exchange IPv4 routes and MPLS labels. This configuration procedure uses ASBR1 as an example.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **send-label**
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                  |
| Step 4 | <b>neighbor {ip-address   peer-group-name} remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor hh.0.0.1 remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                                                     |
| Step 5 | <b>address-family ipv4 [multicast   unicast   mdt   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4          | Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>mdt</b> keyword specifies an IPv4 multicast distribution tree (MDT) address family session.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor hh.0.0.1<br>activate | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 7 | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor hh.0.0.1<br>send-label                             | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                     |
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                  | Exits address family configuration mode.                                                                                                                                                                                                                                       |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                  | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                      |

## Configuring the Route Reflectors to Exchange VPN-IPv4 Routes

Perform this task to enable the route reflectors to exchange VPN-IPv4 routes by using multihop, multiprotocol eBGP.

This procedure also specifies that the next hop information and the VPN label are to be preserved across the autonomous systems. This procedure uses RR1 as an example of the route reflector.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family vpnv4** [unicast]
6. **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*tth*]
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **next-hop unchanged**
9. **exit-address-family**
10. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                       | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> The autonomous system number identifies RR1 to routers in other autonomous systems. |
| Step 4 | <b>neighbor {ip-address   peer-group-name} remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor bb.bb.bb.bb remote-as 200     | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                        |
| Step 5 | <b>neighbor {ip-address   peer-group-name} ebgp-multihop [ttl]</b><br><br><b>Example:</b><br>Router(config-router)# neighbor bb.bb.bb.bb ebgp-multihop 255 | Accepts and attempts BGP connections to external peers residing on networks that are not directly connected. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>ttl</i> argument specifies the time-to-live in the range from 1 to 255 hops.</li> </ul>                                                                                                     |
| Step 6 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                | Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                                                                                                                 |

|         | Command or Action                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                 |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor bb.bb.bb.bb activate                    | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                          |
| Step 8  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>next-hop unchanged</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ip-address next-hop unchanged | Enables an eBGP multihop peer to propagate the next hop unchanged. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the next hop.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group that is the next hop.</li> </ul> |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                     | Exits address family configuration mode.                                                                                                                                                                                                                                                                |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                        | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                               |

## Configuring the Route Reflector to Reflect Remote Routes in Its Autonomous System

Perform this task to enable the RR to reflect the IPv4 routes and labels learned by the ASBR to the PE routers in the autonomous system.

This is accomplished by making the ASBR and PE router route reflector clients of the RR. This procedure also explains how to enable the RR to reflect the VPN-IPv4 routes.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **activate**
6. **neighbor** *ip-address* **route-reflector-client**
7. **neighbor** *ip-address* **send-label**
8. **exit-address-family**
9. **address-family vpnv4** [**unicast**]
10. **neighbor** {*ip-address* | *peer-group-name*} **activate**

11. **neighbor *ip-address* route-reflector-client**
12. **exit-address-family**
13. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 3 | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                       | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                           |
| Step 4 | <b>address-family ipv4 [<i>multicast</i>   <i>unicast</i>   <i>vrf vrf-name</i>]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4         | Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard IPv4 address prefixes. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf <i>vrf-name</i></b> keyword and argument specify the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>}</b><br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ee.ee.ee.ee activate | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                   |
| Step 6 | <b>neighbor <i>ip-address</i> route-reflector-client</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ee.ee.ee.ees route-reflector-client         | Configures the router as a BGP route reflector and configures the specified neighbor as its client. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP neighbor being configured as a client.</li> </ul>                                                                                                                                                                                                                                                                  |

|         | Command or Action                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                        |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ee.ee.ee.ee send-label                          | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                     |
| Step 8  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                               | Exits address family configuration mode.                                                                                                                                                                                                                                       |
| Step 9  | <b>address-family</b> <b>vpnvp4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpnvp4                                    | Enters address family configuration mode for configuring routing sessions, such as BGP sessions, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>     |
| Step 10 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ee.ee.ee.ee activate | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 11 | <b>neighbor</b> <i>ip-address</i> <b>route-reflector-client</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor ee.ee.ee.ee route-reflector-client  | Enables the RR to pass iBGP routes to the neighboring router.                                                                                                                                                                                                                  |
| Step 12 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                               | Exits address family configuration mode.                                                                                                                                                                                                                                       |
| Step 13 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                               | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                      |

## Verifying the MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels Configuration

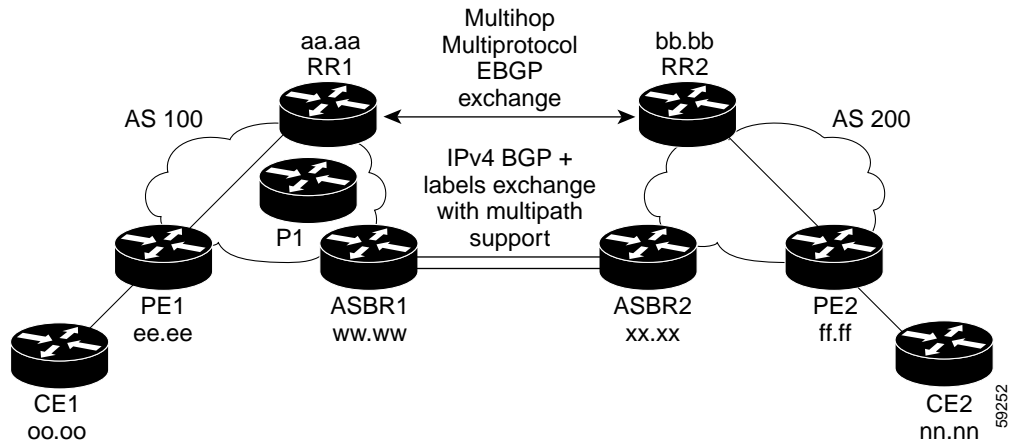
If you use ASBRs to distribute the IPv4 labels and route reflectors to distribute the VPN-IPv4 routes, use the following procedures to help verify the configuration:

- Verifying the Route Reflector Configuration, page 14
- Verifying that CE1 Can Communicate with CE2, page 15
- Verifying that PE1 Can Communicate with CE2, page 16
- Verifying that PE2 Can Communicate with CE2, page 18

- [Verifying the ASBR Configuration, page 19](#)

Figure 3 shows the configuration that is referred to in the next several sections.

**Figure 3** *Configuring Two VPN Service Providers to Exchange IPv4 Routes and MPLS Labels*



## Verifying the Route Reflector Configuration

Perform this task to verify the route reflector configuration.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [summary] [labels]**
3. **disable**

DETAILED STEPS

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all summary | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>summary</b> keywords to verify that a multihop, multiprotocol eBGP session exists between the route reflectors and that the VPNv4 routes are being exchanged between the route reflectors.</li> </ul> <p>The last two lines of the command output show the following information:</p> <ul style="list-style-type: none"> <li>Prefixes are being learned from PE1 and then passed to RR2.</li> <li>Prefixes are being learned from RR2 and then passed to PE1.</li> </ul> <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>labels</b> keywords to verify that the route reflectors exchange VPNv4 label information.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                  | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Verifying that CE1 Can Communicate with CE2

Perform this task to verify that router CE1 has NLRI for router CE2.

SUMMARY STEPS

- enable
- show ip route [ip-address [mask] [longer-prefixes]] | [protocol [process-id]] | [list access-list-number | access-list-name]
- disable

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                        |
| Step 2 | <b>show ip route</b> [ <i>ip-address</i> [ <i>mask</i> ]] [ <b>longer-prefixes</b> ]   [ <i>protocol</i> [ <i>process-id</i> ]]   [ <b>list</b> <i>access-list-number</i>   <i>access-list-name</i> ]<br><br><b>Example:</b><br>Router# show ip route nn.nn.nn.nn | Displays the current state of the routing table. <ul style="list-style-type: none"> <li>Use the <i>ip-address</i> argument to verify that CE1 has a route to CE2.</li> <li>Use this command to verify the routes learned by CE1. Make sure that the route for CE2 is listed.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                          | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                               |

## Verifying that PE1 Can Communicate with CE2

Perform this task to verify that router PE1 has NLRI for router CE2.

## SUMMARY STEPS

- enable**
- show ip route vrf** *vrf-name* [**connected**] [*protocol* [*as-number*] [*tag*] [*output-modifiers*]] [**list** *number* [*output-modifiers*]] [**profile**] [**static** [*output-modifiers*]] [**summary** [*output-modifiers*]] [**supernets-only** [*output-modifiers*]] [**traffic-engineering** [*output-modifiers*]]
- show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [*ip-prefix* | *length*] [**longer-prefixes**] [*output-modifiers*] [*network-address* [*mask*]] [**longer-prefixes**] [*output-modifiers*] [**cidr-only**] [*community*] [**community-list**] [**dampened-paths**] [**filter-list**] [**flap-statistics**] [**inconsistent-as**] [**neighbors**] [**paths** [*line*]] [**peer-group**] [**quote-regexp**] [**regexp**] [**summary**] [**tags**]
- show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
- show mpls forwarding-table** [{*network* {*mask* | *length*} | **labels** *label* [-*label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
- show ip bgp** [*network*] [*network-mask*] [**longer-prefixes**]
- show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]
- disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                           |
| Step 2 | <b>show ip route vrf vrf-name</b> [ <b>connected</b> ]<br>[ <b>protocol</b> [ <b>as-number</b> ] [ <b>tag</b> ] [ <b>output-modifiers</b> ]]<br>[ <b>list number</b> [ <b>output-modifiers</b> ]] [ <b>profile</b> ]<br>[ <b>static</b> [ <b>output-modifiers</b> ]] [ <b>summary</b><br>[ <b>output-modifiers</b> ]] [ <b>supernets-only</b><br>[ <b>output-modifiers</b> ]] [ <b>traffic-engineering</b><br>[ <b>output-modifiers</b> ]]<br><br><b>Example:</b><br>Router# show ip route vrf vpn1 nn.nn.nn.nn                                                                                                                                                                                                                                                                          | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use this command to verify that router PE1 learns routes from router CE2 (nn.nn.nn.nn).</li> </ul>                                  |
| Step 3 | <b>show ip bgp vpnv4</b> { <b>all</b>   <b>rd route-distinguisher</b><br>  <b>vrf vrf-name</b> } [ <b>ip-prefix length</b><br>[ <b>longer-prefixes</b> ] [ <b>output-modifiers</b> ]]<br>[ <b>network-address</b> [ <b>mask</b> ] [ <b>longer-prefixes</b> ]<br>[ <b>output-modifiers</b> ]] [ <b>cidr-only</b> ] [ <b>community</b> ]<br>[ <b>community-list</b> ] [ <b>dampened-paths</b> ] [ <b>filter-list</b> ]<br>[ <b>flap-statistics</b> ] [ <b>inconsistent-as</b> ] [ <b>neighbors</b> ]<br>[ <b>paths</b> [ <b>line</b> ]] [ <b>peer-group</b> ] [ <b>quote-regexp</b> ]<br>[ <b>regexp</b> ] [ <b>summary</b> ] [ <b>tags</b> ]<br><br><b>Example:</b><br>Router# show ip bgp vpnv4 vrf vpn1 nn.nn.nn.nn<br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all nn.nn.nn.nn | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>vrf</b> or <b>all</b> keyword to verify that router PE2 is the BGP next-hop to router CE2.</li> </ul>                    |
| Step 4 | <b>show ip cef</b> [ <b>vrf vrf-name</b> ] [ <b>network</b> [ <b>mask</b> ]]<br>[ <b>longer-prefixes</b> ] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show ip cef vrf vpn1 nn.nn.nn.nn                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | (Optional) Displays entries in the Forwarding Information Base (FIB) or displays a summary of the FIB. <ul style="list-style-type: none"> <li>Use this command to verify that the Cisco Express Forwarding entries are correct.</li> </ul> |
| Step 5 | <b>show mpls forwarding-table</b> [{ <b>network</b> { <b>mask</b>  <br><b>length</b> }   <b>labels label</b> [ <b>-label</b> ]   <b>interface</b><br><b>interface</b>   <b>next-hop address</b>   <b>lsp-tunnel</b><br>[ <b>tunnel-id</b> ]}] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show mpls forwarding-table                                                                                                                                                                                                                                                                                                                                                                                                                                                             | (Optional) Displays the contents of the MPLS LFIB. <ul style="list-style-type: none"> <li>Use this command to verify the IGP label for the BGP next hop router (autonomous system boundary).</li> </ul>                                    |
| Step 6 | <b>show ip bgp</b> [ <b>network</b> ] [ <b>network-mask</b> ]<br>[ <b>longer-prefixes</b> ]<br><br><b>Example:</b><br>Router# show ip bgp ff.ff.ff.ff                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | (Optional) Displays entries in the BGP routing table. <ul style="list-style-type: none"> <li>Use the <b>show ip bgp</b> command to verify the label for the remote egress PE router (PE2).</li> </ul>                                      |



|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</pre> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all labels</p> | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>summary</b> keywords to verify the VPN label of CE2, as advertised by PE2.</li> </ul> |
| Step 8 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                 | (Optional) Exits to user EXEC mode.                                                                                                                                                                                    |

## Verifying that PE2 Can Communicate with CE2

Perform this task to ensure that PE2 can access CE2.

### SUMMARY STEPS

1. **enable**
2. **show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]**
3. **show mpls forwarding-table [vrf vrf-name] [{network {mask | length} | labels label [-label] | interface interface | next-hop address | lsp-tunnel [tunnel-id]]] [detail]**
4. **show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [summary] [labels]**
5. **show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]**
6. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <pre>enable</pre> <p><b>Example:</b><br/>Router&gt; enable</p>                                                                                                                                                                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                    |
| Step 2 | <pre>show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]] [list number [output-modifiers]] [profile] [static [output-modifiers]] [summary [output-modifiers]] [supernets-only [output-modifiers]] [traffic-engineering [output-modifiers]]</pre> <p><b>Example:</b><br/>Router# show ip route vrf vpn1 nn.nn.nn.nn</p> | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use this command to check the VPN routing and forwarding table for CE2. The output provides next-hop information.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>show mpls forwarding-table [vrf vrf-name] [{network {mask   length}   labels label [-label]   interface interface   next-hop address   lsp-tunnel {tunnel-id}}] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table vrf vpn1 nn.nn.nn.nn</p> | <p>(Optional) Displays the contents of the LFIB.</p> <ul style="list-style-type: none"> <li>Use the <b>vrf</b> keyword to check the VPN routing and forwarding table for CE2. The output provides the label for CE2 and the outgoing interface.</li> </ul>                           |
| Step 4 | <pre>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</pre> <p><b>Example:</b><br/>Router# show ip bgp vpnv4 all labels</p>                                                                                                          | <p>(Optional) Displays VPN address information from the BGP table.</p> <ul style="list-style-type: none"> <li>Use the <b>all</b> and <b>labels</b> keywords to check the VPN label for CE2 in the multiprotocol BGP table.</li> </ul>                                                |
| Step 5 | <pre>show ip cef [vrf vrf-name] [network {mask}] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef vpn1 nn.nn.nn.nn</p>                                                                                                                      | <p>(Optional) Displays entries in the FIB or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use this command to check the Cisco Express Forwarding entry for CE2. The command output shows the local label for CE2 and the outgoing interface.</li> </ul> |
| Step 6 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                                          | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                                           |

## Verifying the ASBR Configuration

Perform this task to verify that the ASBRs exchange IPv4 routes with MPLS labels or IPv4 routes without labels as prescribed by a route map.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp** [network] [network-mask] [longer-prefixes]
3. **show ip cef** [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]
4. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>show ip bgp</b> [ <i>network</i> ] [ <i>network-mask</i> ]<br>[ <i>longer-prefixes</i> ]<br><br><b>Example:</b><br>Router# show ip bgp ff.ff.ff.ff                                                                                    | (Optional) Displays entries in the BGP routing table. <ul style="list-style-type: none"> <li>Use this command to check that: <ul style="list-style-type: none"> <li>ASBR1 receives an MPLS label for PE2 from ASBR2.</li> <li>ASBR1 receives IPv4 routes for RR2 without labels from ASBR2.</li> <li>ASBR2 distributes an MPLS label for PE2 to ASBR1.</li> <li>ASBR2 does not distribute a label for RR2 to ASBR1.</li> </ul> </li> </ul> |
| Step 3 | <b>show ip cef</b> [ <i>vrf vrf-name</i> ] [ <i>network [mask]</i> ]<br>[ <i>longer-prefixes</i> ] [ <i>detail</i> ]<br><br><b>Example:</b><br>Router# show ip cef ff.ff.ff.ff<br><br><b>Example:</b><br>Router# show ip cef bb.bb.bb.bb | (Optional) Displays entries in the FIB or displays a summary of the FIB. <ul style="list-style-type: none"> <li>Use this command from ASBR1 and ASBR2 to check that: <ul style="list-style-type: none"> <li>The Cisco Express Forwarding entry for PE2 is correct.</li> <li>The Cisco Express Forwarding entry for RR2 is correct.</li> </ul> </li> </ul>                                                                                  |
| Step 4 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                 | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                        |

## Configuration Examples for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Configuration examples for MPLS VPN Inter-AS are as follows:

- Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over an MPLS VPN Service Provider: Examples, page 20
- Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Examples, page 26

## Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over an MPLS VPN Service Provider: Examples

Configuration examples for Inter-AS using BGP to distribute routes and MPLS labels over an MPLS VPN service provider included in this section are as follows:

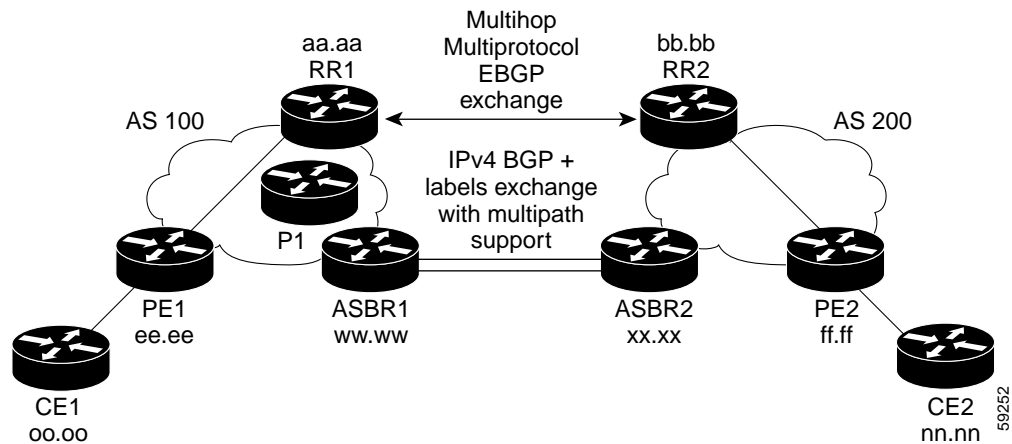
- [Route Reflector 1 Configuration Example \(MPLS VPN Service Provider\)](#), page 22
- [ASBR1 Configuration Example \(MPLS VPN Service Provider\)](#), page 23
- [Route Reflector 2 Configuration Example \(MPLS VPN Service Provider\)](#), page 24
- [ASBR2 Configuration Example \(MPLS VPN Service Provider\)](#), page 25

Figure 4 shows two MPLS VPN service providers. The service provider distributes the VPN-IPv4 routes between the route reflectors. The MPLS VPN service providers distribute the IPv4 routes with MPLS labels between the ASBRs.

The configuration example shows the following two techniques you can use to distribute the VPN-IPv4 routes and the IPv4 routes with MPLS labels of the remote RRs and PEs to the local RRs and PEs:

- Autonomous system 100 uses the RRs to distribute the VPN-IPv4 routes learned from the remote RRs. The RRs also distribute the remote PE address and label learned from ASBR1 using IPv4 labels.
- In Autonomous system 200, the IPv4 routes that ASBR2 learned are redistributed into IGP.

**Figure 4** *Distributing IPv4 Routes and MPLS Labels Between MPLS VPN Service Providers*



## Route Reflector 1 Configuration Example (MPLS VPN Service Provider)

The configuration example for RR1 specifies the following:

- RR1 exchanges VPN-IPv4 routes with RR2 using multiprotocol, multihop eBGP.
- The VPN-IPv4 next-hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1:
  - The VPN-IPv4 routes learned from RR2
  - The IPv4 routes and MPLS labels learned from ASBR1

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet0/3
 ip address dd.0.0.2 255.0.0.0
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor ee.aa.aa.aa remote-as 100
 neighbor ee.aa.aa.aa update-source Loopback0
 neighbor ww.ww.ww.ww remote-as 100
 neighbor ww.ww.ww.ww update-source Loopback0
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb ebgp-multihop 255
 neighbor bb.bb.bb.bb update-source Loopback0
 no auto-summary
!
address-family ipv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client           !IPv4+labels session to PE1
 neighbor ee.aa.aa.aa send-label
 neighbor ww.ww.ww.ww activate
 neighbor ww.ww.ww.ww route-reflector-client           !IPv4+labels session to ASBR1
 neighbor ww.ww.ww.ww send-label
 no neighbor bb.bb.bb.bb activate
 no auto-summary
 no synchronization
 exit-address-family
!
address-family vpnv4
 neighbor ee.aa.aa.aa activate
 neighbor ee.aa.aa.aa route-reflector-client           !VPNV4 session with PE1
 neighbor ee.aa.aa.aa send-community extended
 neighbor bb.bb.bb.bb activate
 neighbor bb.bb.bb.bb next-hop-unchanged               !MH-VPNV4 session with RR2
 neighbor bb.bb.bb.bb send-community extended           !with next hop unchanged
 exit-address-family
!
ip default-gateway 3.3.0.1
```

```

no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## ASBR1 Configuration Example (MPLS VPN Service Provider)

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

In this example, ASBR1 uses route maps to filter routes:

- A route map called OUT specifies that ASBR1 should distribute the PE1 route (ee.ee) with labels and the RR1 route (aa.aa) without labels.
- A route map called IN specifies that ASBR1 should accept the PE2 route (ff.ff) with labels and the RR2 route (bb.bb) without labels.

```

ip subnet-zero
mpls label protocol ldp
!
interface Loopback0
 ip address ww.ww.ww.ww 255.255.255.255
!
interface Ethernet0/2
 ip address hh.0.0.2 255.0.0.0
!
interface Ethernet0/3
 ip address dd.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network ww.ww.ww.ww 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100

router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor hh.0.0.1 remote-as 200
 no auto-summary
!
!
address-family ipv4
 redistribute ospf 10
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa send-label
 neighbor hh.0.0.1 activate
 neighbor hh.0.0.1 advertisement-interval 5
 neighbor hh.0.0.1 send-label
 neighbor hh.0.0.1 route-map IN in
 neighbor hh.0.0.1 route-map OUT out

```

! Redistributing IGP into BGP  
! so that PE1 & RR1 loopbacks  
! get into the BGP table

! accepting routes in route map IN.  
! distributing routes in route map OUT.

```

neighbor kk.0.0.1 activate
neighbor kk.0.0.1 advertisement-interval 5
neighbor kk.0.0.1 send-label
neighbor kk.0.0.1 route-map IN in          ! accepting routes in route map IN.
neighbor kk.0.0.1 route-map OUT out       ! distributing routes in route map OUT.
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.0.0.0 log          !Setting up the access lists
access-list 2 permit ff.0.0.0 log
access-list 3 permit aa.0.0.0 log
access-list 4 permit bb.0.0.0 log

route-map IN permit 10                    !Setting up the route maps
match ip address 2
match mpls-label
!
route-map IN permit 11
match ip address 4
!
route-map OUT permit 12
match ip address 3
!
route-map OUT permit 13
match ip address 1
set mpls-label
!
end

```

## Route Reflector 2 Configuration Example (MPLS VPN Service Provider)

RR2 exchanges VPN-IPv4 routes with RR1 through multihop, multiprotocol eBGP. This configuration also specifies that the next-hop information and the VPN label are preserved across the autonomous systems:

```

ip subnet-zero
ip cef
!
interface Loopback0
 ip address bb.0.0.0 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.0 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.0.0.0 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.0.0.0 remote-as 100
 neighbor aa.0.0.0 ebgp-multihop 255
 neighbor aa.0.0.0 update-source Loopback0
 neighbor ff.0.0.0 remote-as 200
 neighbor ff.0.0.0 update-source Loopback0

```

```

no auto-summary
!
address-family vpnv4
neighbor aa.aa.aa.aa activate
neighbor aa.aa.aa.aa next-hop-unchanged           !Multihop VPNv4 session with RR1
neighbor aa.aa.aa.aa send-community extended      !with next-hop-unchanged
neighbor ff.ff.ff.ff activate
neighbor ff.ff.ff.ff route-reflector-client       !VPNv4 session with PE2
neighbor ff.ff.ff.ff send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end

```

## ASBR2 Configuration Example (MPLS VPN Service Provider)

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```

ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet1/0
 ip address hh.0.0.1 255.0.0.0
!
interface Ethernet1/2
 ip address jj.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
router ospf 20
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 200 subnets           ! Redistributing the routes learned from
 passive-interface Ethernet1/0          ! ASBR1(eBGP+labels session) into IGP
 network xx.xx.xx.xx 0.0.0.0 area 200    ! so that PE2 will learn them
 network jj..0.0 0.255.255.255 area 200
!
router bgp 200
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor bb.bb.bb.bb remote-as 200
 neighbor bb.bb.bb.bb update-source Loopback0
 neighbor hh.0.0.2 remote-as 100
 no auto-summary
!
address-family ipv4
 redistribute ospf 20                   ! Redistributing IGP into BGP
 neighbor hh.0.0.2 activate             ! so that PE2 & RR2 loopbacks
 neighbor hh.0.0.2 advertisement-interval 5 ! will get into the BGP-4 table.
 neighbor hh.0.0.2 route-map IN in
 neighbor hh.0.0.2 route-map OUT out
 neighbor hh.0.0.2 send-label

```



```

neighbor kk.0.0.2 activate
neighbor kk.0.0.2 advertisement-interval 5
neighbor kk.0.0.2 route-map IN in
neighbor kk.0.0.2 route-map OUT out
neighbor kk.0.0.2 send-label
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log           !Setting up the access lists
access-list 2 permit ee.aa.aa.aa log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log

route-map IN permit 11                         !Setting up the route maps
match ip address 2
match mpls-label
!
route-map IN permit 12
match ip address 4
!
route-map OUT permit 10
match ip address 1
set mpls-label
!
route-map OUT permit 13
match ip address 3
end

```

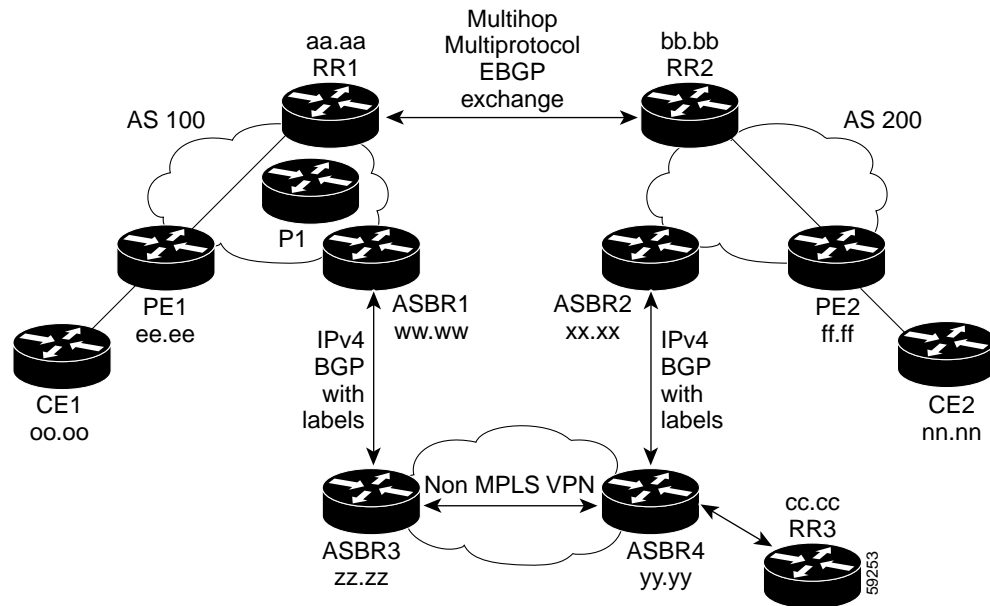
## Configuring MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Examples

Configuration examples for Inter-AS using BGP to distribute routes and MPLS labels over a non MPLS VPN service provider included in this section are as follows:

- [Route Reflector 1 Configuration Example \(Non-MPLS VPN Service Provider\), page 27](#)
- [ASBR1 Configuration Example \(Non-MPLS VPN Service Provider\), page 28](#)
- [Route Reflector 2 Configuration Example \(Non-MPLS VPN Service Provider\), page 30](#)
- [ASBR2 Configuration Example \(Non-MPLS VPN Service Provider\), page 30](#)
- [ASBR3 Configuration Example \(Non-MPLS VPN Service Provider\), page 32](#)
- [Route Reflector 3 Configuration Example \(Non-MPLS VPN Service Provider\), page 33](#)
- [ASBR4 Configuration Example \(Non-MPLS VPN Service Provider\), page 34](#)

Figure 5 shows two MPLS VPN service providers that are connected through a non MPLS VPN service provider. The autonomous system in the middle of the network is configured as a backbone autonomous system that uses LDP or Tag Distribution Protocol (TDP) to distribute MPLS labels. Traffic engineering tunnels can also be used instead of TDP or LDP to build the LSP across the non MPLS VPN service provider.

**Figure 5** *Distributing Routes and MPLS Labels over a Non-MPLS VPN Service Provider*



## Route Reflector 1 Configuration Example (Non-MPLS VPN Service Provider)

The configuration example for RR1 specifies the following:

- RR1 exchanges VPN-IPv4 routes with RR2 using multiprotocol, multihop eBGP.
- The VPN-IPv4 next-hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1:
  - The VPN-IPv4 routes learned from RR2
  - The IPv4 routes and MPLS labels learned from ASBR1

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
 ip address dd.0.0.2 255.0.0.0
 clockrate 124061
!
router ospf 10
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network aa.aa.aa.aa 0.0.0.0 area 100
 network dd.0.0.0 0.255.255.255 area 100
```

```

!
router bgp 100
  bgp cluster-id 1
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor ee.aa.aa.aa remote-as 100
  neighbor ee.aa.aa.aa update-source Loopback0
  neighbor ww.ww.ww.ww remote-as 100
  neighbor ww.ww.ww.ww update-source Loopback0
  neighbor bb.bb.bb.bb remote-as 200
  neighbor bb.bb.bb.bb ebgp-multihop 255
  neighbor bb.bb.bb.bb update-source Loopback0
  no auto-summary
!
address-family ipv4
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa route-reflector-client           !IPv4+labels session to PE1
  neighbor ee.aa.aa.aa send-label
  neighbor ww.ww.ww.ww activate
  neighbor ww.ww.ww.ww route-reflector-client           !IPv4+labels session to ASBR1
  neighbor ww.ww.ww.ww send-label
  no neighbor bb.bb.bb.bb activate
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa route-reflector-client           !VPNv4 session with PE1
  neighbor ee.aa.aa.aa send-community extended
  neighbor bb.bb.bb.bb activate
  neighbor bb.bb.bb.bb next-hop-unchanged               !MH-VPNv4 session with RR2
  neighbor bb.bb.bb.bb send-community extended           with next-hop-unchanged
  exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## ASBR1 Configuration Example (Non-MPLS VPN Service Provider)

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

In this example, ASBR1 uses route maps to filter routes:

- A route map called OUT specifies that ASBR1 should distribute the PE1 route (ee.aa) with labels and the RR1 route (aa.aa) without labels.
- A route map called IN specifies that ASBR1 should accept the PE2 route (ff.aa) with labels and the RR2 route (bb.bb) without labels.

```

ip subnet-zero
ip cef distributed
mpls label protocol ldp
!
interface Loopback0

```

```

ip address ww.ww.ww.ww 255.255.255.255
!
interface Serial3/0/0
ip address kk.0.0.2 255.0.0.0
ip route-cache distributed
!
interface Ethernet0/3
ip address dd.0.0.1 255.0.0.0
mpls label protocol ldp
mpls ip
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Serial3/0/0
network ww.ww.ww.ww 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100

router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa update-source Loopback0
neighbor kk.0.0.1 remote-as 200
no auto-summary
!
address-family ipv4
redistribute ospf 10                                ! Redistributing IGP into BGP
neighbor aa.aa.aa.aa activate                        ! so that PE1 & RR1 loopbacks
neighbor aa.aa.aa.aa send-label                     ! get into BGP table
neighbor kk.0.0.1 activate
neighbor kk.0.0.1 advertisement-interval 5
neighbor kk.0.0.1 send-label
neighbor kk.0.0.1 route-map IN in                   ! Accepting routes specified in route map IN
neighbor kk.0.0.1 route-map OUT out                 ! Distributing routes specified in route map OUT
no auto-summary
no synchronization
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ee.aa.aa.aa log
access-list 2 permit ff.aa.aa.aa log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.aa.aa.aa log
!
route-map IN permit 10
match ip address 2
match mpls-label
!
route-map IN permit 11
match ip address 4
!
route-map OUT permit 12
match ip address 3
!
route-map OUT permit 13
match ip address 1
set mpls-label
!
end

```

## Route Reflector 2 Configuration Example (Non-MPLS VPN Service Provider)

RR2 exchanges VPN-IPv4 routes with RR1 using multihop, multiprotocol eBGP. This configuration also specifies that the next-hop information and the VPN label are preserved across the autonomous systems:

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
 ip address ii.0.0.2 255.0.0.0
!
router ospf 20
 log-adjacency-changes
 network bb.bb.bb.bb 0.0.0.0 area 200
 network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
 bgp cluster-id 1
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor aa.aa.aa.aa remote-as 100
 neighbor aa.aa.aa.aa ebgp-multihop 255
 neighbor aa.aa.aa.aa update-source Loopback0
 neighbor ff.ff.ff.ff remote-as 200
 neighbor ff.ff.ff.ff update-source Loopback0
 no auto-summary
!
address-family vpnv4
 neighbor aa.aa.aa.aa activate
 neighbor aa.aa.aa.aa next-hop-unchanged           !MH vpnv4 session with RR1
 neighbor aa.aa.aa.aa send-community extended      !with next-hop-unchanged
 neighbor ff.ff.ff.ff activate
 neighbor ff.ff.ff.ff route-reflector-client        !vpnv4 session with PE2
 neighbor ff.ff.ff.ff send-community extended
 exit-address-family
!
ip default-gateway 3.3.0.1
no ip classless
!
end
```

## ASBR2 Configuration Example (Non-MPLS VPN Service Provider)

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```
ip subnet-zero
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet0/1
 ip address qq.0.0.2 255.0.0.0
!
interface Ethernet1/2
```

```

ip address jj.0.0.1 255.0.0.0
mpls label protocol ldp
mpls ip
!
router ospf 20
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets
redistribute bgp 200 subnets          !redistributing the routes learned from
passive-interface Ethernet0/1         !ASBR2 (eBGP+labels session) into IGP
network xx.xx.xx.xx 0.0.0.0 area 200   !so that PE2 will learn them
network jj.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
neighbor qq.0.0.1 remote-as 100
no auto-summary
!
address-family ipv4          ! Redistributing IGP into BGP
redistribute ospf 20          ! so that PE2 & RR2 loopbacks
neighbor qq.0.0.1 activate    ! will get into the BGP-4 table
neighbor qq.0.0.1 advertisement-interval 5
neighbor qq.0.0.1 route-map IN in
neighbor qq.0.0.1 route-map OUT out
neighbor qq.0.0.1 send-label
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 11
match ip address 2
match mpls-label
!
route-map IN permit 12
match ip address 4
!
route-map OUT permit 10
match ip address 1
set mpls-label
!
route-map OUT permit 13
match ip address 3
!
end

```

## ASBR3 Configuration Example (Non-MPLS VPN Service Provider)

ASBR3 belongs to a non MPLS VPN service provider. ASBR3 exchanges IPv4 routes and MPLS labels with ASBR1. ASBR3 also passes the routes learned from ASBR1 to ASBR3 through RR3.



### Note

Do not redistribute eBGP routes learned into iBGP if you are using iBGP to distribute the routes and labels. This is not a supported configuration.

```
ip subnet-zero
ip cef
!
interface Loopback0
 ip address yy.yy.yy.yy 255.255.255.255
interface Hssi4/0
 ip address mm.0.0.0.1 255.0.0.0
 mpls ip
 hssi internal-clock
!
interface Serial5/0
 ip address kk.0.0.1 255.0.0.0
 load-interval 30
 clockrate 124061
!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 network yy.yy.yy.yy 0.0.0.0 area 300
 network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor kk.0.0.2 remote-as 100
 no auto-summary
!
 address-family ipv4
  neighbor cc.cc.cc.cc activate ! iBGP+labels session with RR3
  neighbor cc.cc.cc.cc send-label
  neighbor kk.0.0.2 activate ! eBGP+labels session with ASBR1
  neighbor kk.0.0.2 advertisement-interval 5
  neighbor kk.0.0.2 send-label
  neighbor kk.0.0.2 route-map IN in
  neighbor kk.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit ee.aa.aa.aa log
access-list 2 permit ff.aa.aa.aa log
access-list 3 permit aa.aa.aa.aa log
access-list 4 permit bb.bb.bb.bb log
!
route-map IN permit 10
 match ip address 1
 match mpls-label
!
```

```

route-map IN permit 11
  match ip address 3
!
route-map OUT permit 12
  match ip address 2
  set mpls-label
!
route-map OUT permit 13
  match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end

```

## Route Reflector 3 Configuration Example (Non-MPLS VPN Service Provider)

RR3 is a non MPLS VPN RR that reflects IPv4 routes with MPLS labels to ASBR3 and ASBR4.

```

ip subnet-zero
mpls label protocol ldp
mpls traffic-eng auto-bw timers
no mpls ip
!
interface Loopback0
  ip address cc.cc.cc.cc 255.255.255.255
!
interface POS0/2
  ip address pp.0.0.1 255.0.0.0
  crc 16
  clock source internal
!
router ospf 30
  log-adjacency-changes
  network cc.cc.cc.cc 0.0.0.0 area 300
  network pp.0.0.0 0.255.255.255 area 300
!
router bgp 300
  bgp log-neighbor-changes
  neighbor zz.zz.zz.zz remote-as 300
  neighbor zz.zz.zz.zz update-source Loopback0
  neighbor yy.yy.yy.yy remote-as 300
  neighbor yy.yy.yy.yy update-source Loopback0
  no auto-summary
!
address-family ipv4
  neighbor zz.zz.zz.zz activate
  neighbor zz.zz.zz.zz route-reflector-client
  neighbor zz.zz.zz.zz send-label ! iBGP+labels session with ASBR3
  neighbor yy.yy.yy.yy activate
  neighbor yy.yy.yy.yy route-reflector-client
  neighbor yy.yy.yy.yy send-label ! iBGP+labels session with ASBR4
  no auto-summary
  no synchronization
  exit-address-family
!
ip default-gateway 3.3.0.1
ip classless
!
end

```



## ASBR4 Configuration Example (Non-MPLS VPN Service Provider)

ASBR4 belongs to a non MPLS VPN service provider. ASBR4 and ASBR3 exchange IPv4 routes and MPLS labels by means of RR3.



### Note

Do not redistribute eBGP routes learned into iBGP if you are using iBGP to distribute the routes and labels. This is not a supported configuration.

```
ip subnet-zero
ip cef distributed
!
interface Loopback0
 ip address zz.zz.zz.zz 255.255.255.255
!
interface Ethernet0/2
 ip address qq.0.0.1 255.0.0.0
!
interface POS1/1/0
 ip address pp.0.0.2 255.0.0.0
 ip route-cache distributed
!
interface Hssi2/1/1
 ip address mm.0.0.2 255.0.0.0
 ip route-cache distributed
 mpls label protocol ldp
 mpls ip
 hssi internal-clock
!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet0/2
 network zz.zz.zz.zz 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
 network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor qq.0.0.2 remote-as 200
 no auto-summary
!
 address-family ipv4
  neighbor cc.cc.cc.cc activate
  neighbor cc.cc.cc.cc send-label
  neighbor qq.0.0.2 activate
  neighbor qq.0.0.2 advertisement-interval 5
  neighbor qq.0.0.2 send-label
  neighbor qq.0.0.2 route-map IN in
  neighbor qq.0.0.2 route-map OUT out
 no auto-summary
 no synchronization
 exit-address-family
!
ip classless
!
access-list 1 permit ff.ff.ff.ff log
access-list 2 permit ee.ee.ee.ee log
```

```
access-list 3 permit bb.bb.bb.bb log
access-list 4 permit aa.aa.aa.aa log
!
route-map IN permit 10
  match ip address 1
  match mpls-label
!
route-map IN permit 11
  match ip address 3
!
route-map OUT permit 12
  match ip address 2
  set mpls-label
!
route-map OUT permit 13
  match ip address 4
!
ip default-gateway 3.3.0.1
ip classless
!
end
```

## Command Reference

This feature uses no new or modified commands.

# Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                         |
|----------|---------------------------------------------------------------|
| RFC 1700 | <i>Assigned Numbers</i>                                       |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i> |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                  |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                     |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                    |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

[Table 2](#) lists the features in this module and provides links to specific configuration information.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



### Note

[Table 2](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

| Feature Name                                                        | Releases                                                                                              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels | 12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.0(24)S<br>12.2(14)S<br>12.0(27)S<br>12.0(29)S | <p>This module explains how to configure an MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol, external Border Gateway Protocol (eBGP).</p> <p>This feature uses no new or modified commands.</p> |

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP,

CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

© 2005–2008 Cisco Systems, Inc. All rights reserved.







# MPLS VPN Carrier Supporting Carrier Using LDP and an IGP

---

**First Published:** May 2, 2005  
**Last Updated:** February 5, 2009

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. This module explains how to configure the MPLS VPN CSC network using MPLS Label Distribution Protocol (LDP) to distribute MPLS labels and an Interior Gateway Protocol (IGP) to distribute routes.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS VPN CSC with LDP and IGP](#)” section on page 66.

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

## Contents

- [Prerequisites for MPLS VPN CSC with LDP and IGP](#), page 2
- [Restrictions for MPLS VPN CSC with LDP and IGP](#), page 2
- [Information About MPLS VPN CSC with LDP and IGP](#), page 3
- [How to Configure MPLS VPN CSC with LDP and IGP](#), page 9
- [Configuration Examples for MPLS VPN CSC with LDP and IGP](#), page 18
- [Additional References](#), page 64



---

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



- [Command Reference, page 65](#)
- [Feature Information for MPLS VPN CSC with LDP and IGP, page 66](#)
- [Glossary, page 66](#)

## Prerequisites for MPLS VPN CSC with LDP and IGP

This feature includes the following requirements:

- The provider edge (PE) routers of the backbone carrier require 128 MB of memory.
- The backbone carrier must enable the PE router to check that the packets it receives from the customer edge (CE) router contain only the labels that the PE router advertised to the CE router. This prevents data spoofing, which occurs when a packet from an unrecognized IP address is sent to a router.

## Restrictions for MPLS VPN CSC with LDP and IGP

The following features are not supported with this feature:

- ATM MPLS
- Carrier supporting carrier traffic engineering
- Carrier supporting carrier quality of service (QoS)
- RSVP aggregation
- VPN Multicast between the customer carrier and the backbone carrier network

The following router platforms are supported on the edge of the MPLS VPN:

- Cisco 7200 series
- Cisco 7500 series
- Cisco 12000 series

See [Table 1](#) for Cisco 12000 series line card support added for Cisco IOS releases.

**Table 1** *Cisco12000 Series Line Card Support Added for Cisco IOS Releases*

| Type                    | Line Cards           | Cisco IOS Release Added |
|-------------------------|----------------------|-------------------------|
| Packet over SONET (POS) | 4-Port OC-3 POS      | 12.0(16)ST              |
|                         | 1-Port OC-12 POS     |                         |
|                         | 8-Port OC-3 POS      | 12.0(21)ST              |
|                         | 16-Port OC-3 POS     |                         |
|                         | 4-Port OC-12 POS     |                         |
|                         | 1-Port OC-48 POS     |                         |
|                         | 4-Port OC-3 POS ISE  | 12.0(22)S               |
|                         | 8-Port OC-3 POS ISE  |                         |
|                         | 16 x OC-3 POS ISE    |                         |
|                         | 4 Port OC-12 POS ISE |                         |
|                         | 1-Port OC-48 POS ISE |                         |

**Table 1** Cisco 12000 Series Line Card Support Added for Cisco IOS Releases

| Type                  | Line Cards                                                                                                                       | Cisco IOS Release Added |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| Electrical Interface  | 6- Port DS3                                                                                                                      | 12.0(16)ST              |
|                       | 12- Port DS3<br>6-Port E3                                                                                                        | 12.0(21)ST              |
| ATM                   | 4-Port OC-3 ATM<br>1-Port OC12 ATM<br>4-Port OC-12 ATM                                                                           | 12.0(22)S               |
| Channelized Interface | 2-Port CHOC-3<br>6-Port Ch T3 (DS1)<br>1-Port CHOC-12 (DS3)<br>1-Port CHOC-12 (OC-3)<br>4-Port CHOC-12 ISE<br>1-Port CHOC-48 ISE | 12.0(22)S               |

## Information About MPLS VPN CSC with LDP and IGP

Before configuring MPLS VPN CSC, you should understand the following concepts:

- [MPLS VPN CSC Introduction, page 3](#)
- [Benefits of Implementing MPLS VPN CSC, page 3](#)
- [Configuration Options for MPLS VPN CSC with LDP and IGP, page 4](#)

## MPLS VPN CSC Introduction

Carrier supporting carrier is where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

A backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier can be either:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

## Benefits of Implementing MPLS VPN CSC

The MPLS VPN CSC provides the following benefits to service providers who are backbone carriers and to customer carriers.

### Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the

backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.

- The MPLS VPN carrier supporting carrier feature is scalable. Carrier supporting carrier can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The carrier supporting carrier feature enables tens of thousands of VPNs to be configured over the same network, and it allows a service provider to offer both VPN and Internet services.
- The MPLS VPN carrier supporting carrier feature is a flexible solution. The backbone carrier can accommodate many types of customer carriers. The backbone carrier can accept customer carriers who are ISPs or VPN service providers or both. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

#### **Benefits to the Customer Carriers**

- The MPLS VPN carrier supporting carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide. Customer carriers can also use IPSec in their VPNs for a higher level of security; it is completely transparent to the backbone carrier.
- Customer carriers can use any link layer technology (SONET, Digital Subscriber Line, Frame Relay, and so on) to connect the CE routers to the PE routers and the PE routers to the P routers. The MPLS VPN carrier supporting carrier feature is link layer independent. The CE routers and PE routers use IP to communicate, and the backbone carrier uses MPLS.
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

## **Configuration Options for MPLS VPN CSC with LDP and IGP**

The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be one of the two types of service providers described in the following sections, which explain how the backbone and customer carriers distribute IPv4 routes and MPLS labels.

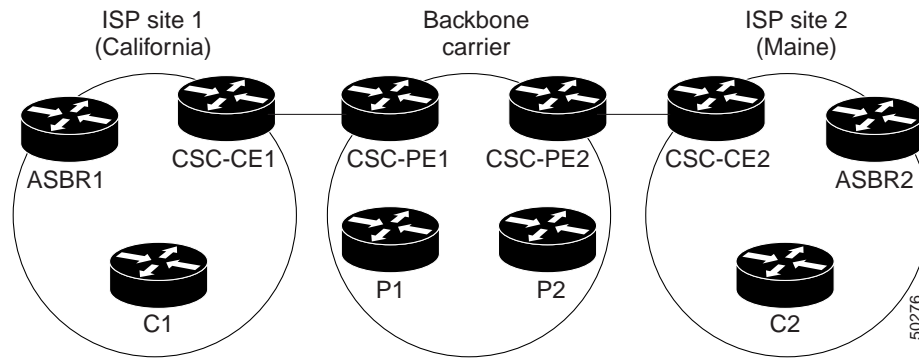
- [Customer Carrier Is an ISP, page 4](#)
- [Customer Carrier Is a BGP/MPLS VPN Service Provider, page 7](#)

### **Customer Carrier Is an ISP**

This section explains how a BGP/MPLS VPN service provider (backbone carrier) can provide a segment of its backbone network to a customer who is an ISP.

Consider the following example:

An ISP has two sites: one in California, the other in Maine. Each site is a point of presence (POP). The ISP wants to connect these sites using a VPN service provided by a backbone carrier. [Figure 1](#) illustrates this situation.

**Figure 1**      **Sample BGP/MPLS Backbone Carrier Supporting an ISP****Note**

The CE routers in the figures are CE routers to the backbone carrier. However, they are PE routers to the customer carrier.

In this example, only the backbone carrier uses MPLS. The customer carrier (ISP) uses only IP. As a result, the backbone carrier must carry all the Internet routes of the customer carrier, which could be as many as 100,000 routes. This poses a scalability problem for the backbone carrier. To solve the scalability problem, the backbone carrier is configured as follows:

- The backbone carrier allows only internal routes of the customer carrier (IGP routes) to be exchanged between the CE routers of the customer carrier and the PE routers of the backbone carrier.
- MPLS is enabled on the interface between the CE router of the customer carrier and the PE router of the backbone carrier.

Internal and external routes are differentiated this way:

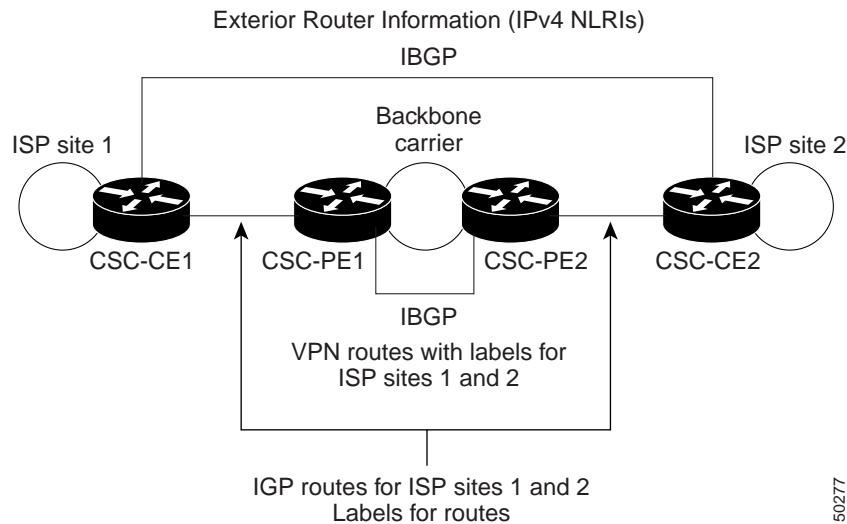
- Internal routes go to any of the routers within the ISP.
- External routes go to the Internet.

The number of internal routes is much lower than the number of external routes. Restricting the routes between the CE routers of the customer carrier and the PE routers of the backbone carrier significantly reduces the number of routes that the PE router needs to maintain.

Because the PE routers do not have to carry external routes in the VRF routing table, they can use the incoming label in the packet to forward the customer carrier Internet traffic. Adding MPLS to the routers provides a consistent method of transporting packets from the customer carrier to the backbone carrier. MPLS allows the exchange of an MPLS label between the PE and the CE routers for every internal customer carrier route. The routers in the customer carrier have all the external routes either through internal Border Gateway Protocol (iBGP) or route redistribution to provide Internet connectivity.

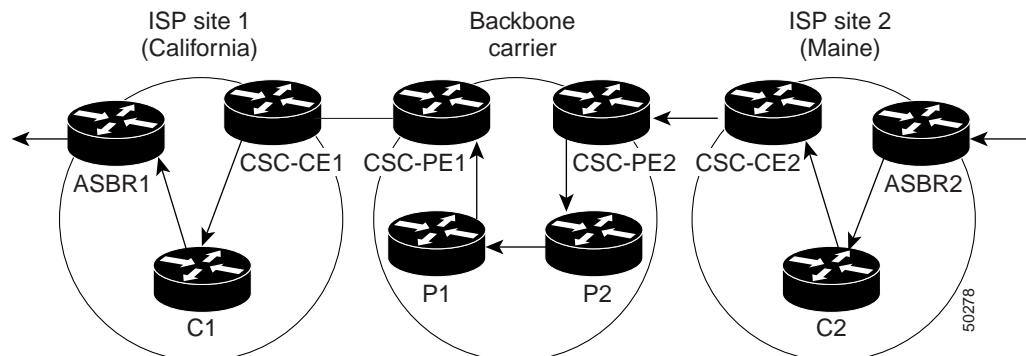
[Figure 2](#) shows how information is exchanged when the network is configured in this manner.

**Figure 2** *Backbone Carrier Exchanging Routing Information with a Customer Carrier Who Is an ISP*



In [Figure 3](#), routes are created between the backbone carrier and the customer carrier sites. ASBR2 receives an Internet route that originated outside the network. All routers in the ISP sites have all the external routes through IBGP connections among them.

**Figure 3** *Establishing a Route Between a Backbone Carrier and a Customer Carrier Who Is an ISP*



[Table 2](#) describes the process of establishing the route, which can be divided into two distinct steps:

- The backbone carrier propagates the IGP information of the customer carrier, which enables the customer carrier routers to reach all the customer carrier routers in the remote sites.
- Once the routers of the customer carriers in different sites are reachable, external routes can be propagated in the customer carrier sites, using IBGP without using the backbone carrier routers.

**Table 2**      ***Establishing a Route Between the Backbone Carrier and the Customer Carrier ISP***

| Step | Description                                                                                                                                                                                                                                                                           |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | CSC-CE2 sends the internal routes within site 2 to CSC-PE2. The routes include the route to ASBR2.                                                                                                                                                                                    |
| 2    | CSC-PE2 sends the routing information for site 2 to CSC-PE1, using MPLS VPN processes. CSC-PE1 gets one label (called L3), which is associated with the route to the VPN-IP address for ASBR2. CSC-PE1 gets another label (called L2), which is associated with the route to CSC-PE2. |
| 3    | CSC-PE1 sends the routing information associated with internal routes from site 2 to CSC-CE1. CSC-PE1 also sends the label binding information. As a result, CSC-CE1 gets the route to ASBR2 with CSC-PE1 as the next hop. The label associated with that route is called L1.         |
| 4    | CSC-CE1 distributes the routing information through site 1. Every router in site 1 gets a route for every internal destination in site 2. Therefore, every router in site 1 can reach routers in site 2 and learn external routes through IBGP.                                       |
| 5    | ASBR2 receives an Internet route.                                                                                                                                                                                                                                                     |
| 6    | The IBGP sessions exchange the external routing information of the ISP, including a route to the Internet. Every router in site 1 knows a route to the Internet, with ASBR2 as the next hop of that route.                                                                            |

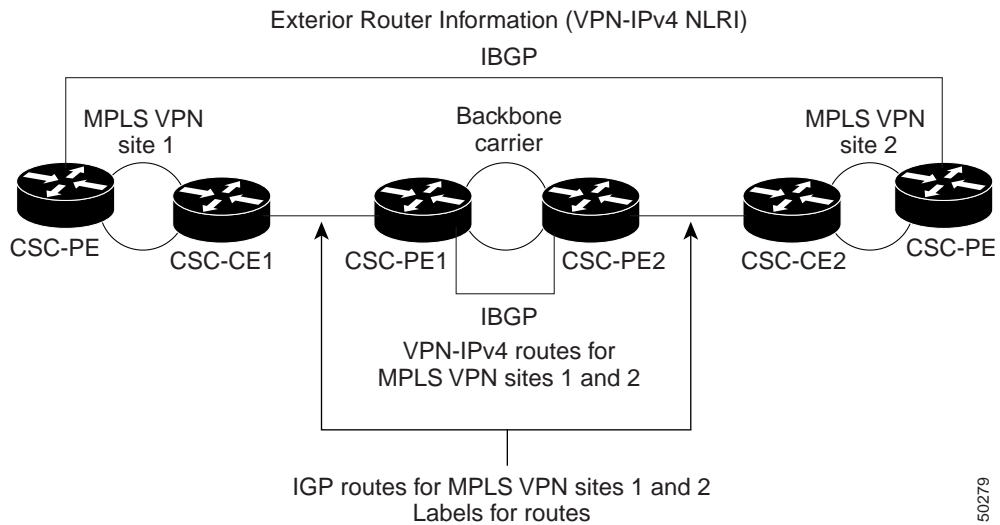
## Customer Carrier Is a BGP/MPLS VPN Service Provider

When a backbone carrier and the customer carrier both provide BGP/MPLS VPN services, the method of transporting data is different from when a customer carrier provides only ISP services. The following list highlights those differences:

- When a customer carrier provides BGP/MPLS VPN services, its external routes are VPN-IPv4 routes. When a customer carrier is an ISP, its external routes are IP routes.
- When a customer carrier provides BGP/MPLS VPN services, every site within the customer carrier must use MPLS. When a customer carrier is an ISP, the sites do not need to use MPLS.

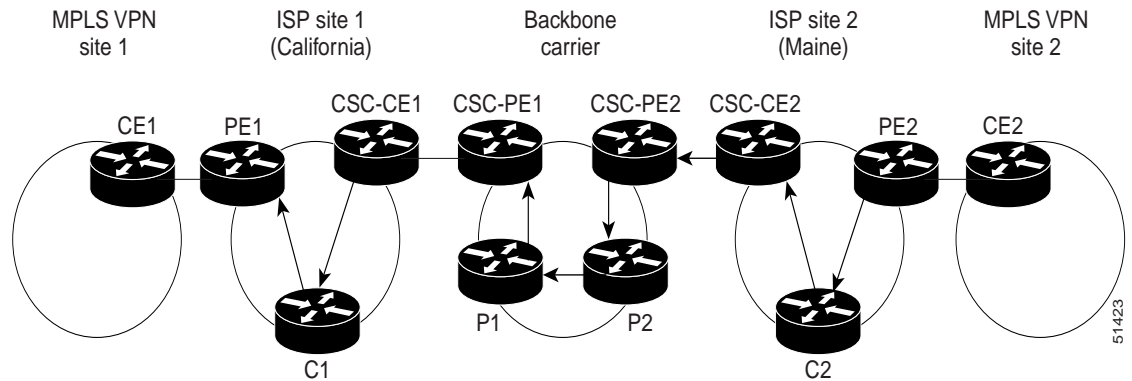
Figure 4 shows how information is exchanged when MPLS VPN services reside on all customer carrier sites and on the backbone carrier.

**Figure 4** Backbone Carrier Exchanging Information with a Customer Carrier Who Is an MPLS VPN Service Provider



In the example shown in [Figure 5](#), routes are created between the backbone carrier and the customer carrier sites.

**Figure 5** Establishing a Route Between a Backbone Carrier and a Customer Carrier Who Is an MPLS VPN Service Provider



[Table 3](#) describes the process of establishing the route.

**Table 3** Establishing a Route Between the Backbone Carrier and Customer Carrier Site

| Step | Description                                                                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | CE2 sends all the internal routes within site 2 to CSC-PE2.                                                                                                                                                                                                                         |
| 2    | CSC-PE2 sends the routing information for site 2 to CSC-PE1, using MPLS VPN processes. CSC-PE1 gets one label (called L3), which is associated with the route to the VPN-IP address for PE2. CSC-PE1 gets another label (called L2), which is associated with the route to CSC-PE2. |

**Table 3**      **Establishing a Route Between the Backbone Carrier and Customer Carrier Site**

| Step | Description                                                                                                                                                                                                                                                                 |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3    | CSC-PE1 sends the routing information associated with internal routes from site 2 to CSC-CE1. CSC-PE1 also sends the label binding information. As a result, CSC-CE1 gets the route to PE2 with CSC-PE1 as the next hop. The label associated with that route is called L1. |
| 4    | CE1 distributes the routing and labeling information through site 1. Every router in site 1 gets a route for every internal destination in site 2. Therefore, PE1 can establish an MP-IBGP session with PE2.                                                                |
| 5    | CE2 advertises the internal routes of MPLS VPN site 2 to PE2.                                                                                                                                                                                                               |
| 6    | PE2 allocates labels for all the VPN routes (regular MPLS VPN functionality) and advertises the labels to PE1, using MP-IBGP.                                                                                                                                               |
| 7    | PE1 can forward traffic from VPN site 1 that is destined for VPN site 2.                                                                                                                                                                                                    |

## How to Configure MPLS VPN CSC with LDP and IGP

This section contains the following procedures:

- [Configuring the Backbone Carrier Core, page 9](#) (required)
- [Configuring the CSC-PE and CSC-CE Routers, page 15](#) (required)
- [Verifying the Carrier Supporting Carrier Configuration, page 17](#) (optional)

### Configuring the Backbone Carrier Core

Configuring the backbone carrier core requires configuring connectivity and routing functions for the CSC core and the CSC-PE routers.

Configuring and verifying the CSC core (backbone carrier) involves the following tasks:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core, page 9](#) (optional)
- [Configuring VRFs for CSC-PE Routers, page 11](#) (required)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier, page 13](#) (required)

### Prerequisites

Before you configure a backbone carrier core, configure the following on the CSC core routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on. For information, see [Configuring a Basic BGP Network](#), [Configuring OSPF](#), [Configuring a Basic IS-IS Network](#), and [Configuring EIGRP](#).
- Label Distribution Protocol (LDP). For information, see [MPLS Label Distribution Protocol](#).

### Verifying IP Connectivity and LDP Configuration in the CSC Core

Perform this task to verify IP connectivity and LDP configuration in the CSC core. For a configuration example for this task, see the [“Verifying IP Connectivity and LDP Configuration in the CSC Core” section on page 9](#).



## SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] [*host-name* | *system-address*]
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]
5. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**]
6. **show mpls ldp neighbor** [[**vrf** *vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf** *vrf-name*] [*interface*] [**detail**] | **all**]
9. **show ip route**
10. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                     |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] [ <i>host-name</i>   <i>system-address</i> ]<br><br><b>Example:</b><br>Router# ping ip 10.0.0.1                                                                                                                                                                                                                                | (Optional) Diagnoses basic network connectivity on AppleTalk, Connectionless Network Service (CLNS), IP, Novell, Apollo, VINES, DECnet, or Xerox Network System (XNS) networks. <ul style="list-style-type: none"> <li>Use the <b>ping ip</b> command to verify the connectivity from one CSC core router to another.</li> </ul>                                     |
| Step 3 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip 10.0.0.1                                                                                                                                                                                                                                                    | (Optional) Discovers the routes that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li> </ul> |
| Step 4 | <b>show mpls forwarding-table</b> [ <i>network</i> { <i>mask</i>   <i>length</i> }   <b>labels</b> <i>label</i> [- <i>label</i> ]   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ]] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show mpls forwarding-table | (Optional) Displays the contents of the MPLS label forwarding information base (LFIB). <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to verify that MPLS packets are being forwarded.</li> </ul>                                                                                                                          |
| Step 5 | <b>show mpls ldp discovery</b> [ <b>vrf</b> <i>vrf-name</i>   <b>all</b> ]<br><br><b>Example:</b><br>Router# show mpls ldp discovery                                                                                                                                                                                                                           | (Optional) Displays the status of the LDP discovery process. <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp discovery</b> command to verify that LDP is operational in the CSC core.</li> </ul>                                                                                                                                                     |

|         | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <pre>show mpls ldp neighbor [[vrf vrf-name] [address   interface] [detail]   all]</pre> <p><b>Example:</b><br/>Router# show mpls ldp neighbor</p> | (Optional) Displays the status of LDP sessions. <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp neighbor</b> command to verify LDP configuration in the CSC core.</li> </ul>                                                                        |
| Step 7  | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef</p>                  | (Optional) Displays entries in the forwarding Information Base (FIB). <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check the forwarding table (prefixes, next hops, and interfaces).</li> </ul>                                     |
| Step 8  | <pre>show mpls interfaces [[vrf vrf-name] [interface] [detail]   all]</pre> <p><b>Example:</b><br/>Router# show mpls interfaces</p>               | (Optional) Displays information about one or more or all interfaces that are configured for label switching. <ul style="list-style-type: none"> <li>Use the <b>show mpls interfaces</b> command to verify that the interfaces are configured to use LDP.</li> </ul> |
| Step 9  | <pre>show ip route</pre> <p><b>Example:</b><br/>Router# show ip route</p>                                                                         | (Optional) Displays IP routing table entries. <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, and interface.</li> </ul>                                       |
| Step 10 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                     | (Optional) Returns to privileged EXEC mode.                                                                                                                                                                                                                         |

## Troubleshooting Tips

You can use the **ping** and **trace** commands to verify complete MPLS connectivity in the core. You also get useful troubleshooting information from the additional **show** commands.

## Configuring VRFs for CSC-PE Routers

Perform this task to configure VPN routing and forwarding (VRF) instances for the backbone carrier edge (CSC-PE) routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **rd route-distinguisher**
5. **route-target {import | export | both} route-target-ext-community**
6. **import map route-map**
7. **exit**
8. **interface type number**
9. **ip vrf forwarding vrf-name**

## 10. end

## DETAILED STEPS

|        | Command or Action                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                            | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 3 | <b>ip vrf vrf-name</b><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1                                                                              | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 4 | <b>rd route-distinguisher</b><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1                                                                      | Creates routing and forwarding tables. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN-IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                                    |
| Step 5 | <b>route-target {import   export   both}</b><br><i>route-target-ext-community</i><br><br><b>Example:</b><br>Router(config-vrf)# route-target import 100:1 | Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6 | <b>import map route-map</b><br><br><b>Example:</b><br>Router(config-vrf)# import map vpn1-route-map                                                       | (Optional) Configures an import route map for a VRF. <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

|         | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                 |
|---------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf)# exit                                               | (Optional) Exits to global configuration mode.                                                                                                                                                                                                                                                          |
| Step 8  | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0          | Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 9  | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                            |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                  | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                               |

### Troubleshooting Tips

Enter a **show ip vrf detail** command and make sure the MPLS VPN is up and associated with the right interfaces.

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier

Perform this task to configure multiprotocol BGP (MP-BGP) for VPN connectivity in the backbone carrier.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*
7. **address-family** **vpn4** [**unicast**]
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community** **extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                   | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast                                                        | (Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>Use the <b>no</b> form of the <b>bgp default-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                                                            |
| Step 5 | <b>neighbor {ip-address   peer-group-name} remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 remote-as 100                    | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                      |
| Step 6 | <b>neighbor {ip-address   peer-group-name} update-source interface-type</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1 update-source loopback0 | Allows BGP sessions to use a specific operational interface for TCP connections. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument specifies the interface to be used as the source.</li> </ul>                              |
| Step 7 | <b>address-family vpnv4 [unicast]</b><br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                            | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                        |

|         | Command or Action                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                               |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>send-community</b> extended<br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>send-community extended | Specifies that a communities attribute should be sent to a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 9  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.12.12.12<br>activate                            | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                    |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                                                | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                             |

### Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command generates an error message, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Configuring the CSC-PE and CSC-CE Routers

To enable the CSC-PE and CSC-CE routers to distribute routes and MPLS labels, perform the following tasks:

- [Configuring LDP on the CSC-PE and CSC-CE Routers, page 15](#) (required)
- [Enabling MPLS Encapsulation on the CSC-PE and CSC-CE Routers, page 16](#) (required)

### Prerequisites

Before you configure the CSC-PE and CSC-CE routers, you must configure an IGP on the CSC-PE and CSC-CE routers. A routing protocol is required between the PE and CE routers that connect the backbone carrier to the customer carrier. The routing protocol enables the customer carrier to exchange IGP routing information with the backbone carrier. Use the same routing protocol that the customer carrier uses. You can choose RIP, OSPF, or static routing as the routing protocol. BGP is not supported. For the configuration steps, see [Configuring MPLS Layer 3 VPNs](#).

### Configuring LDP on the CSC-PE and CSC-CE Routers

MPLS LDP is required between the PE and CE routers that connect the backbone carrier to the customer carrier. You can configure LDP as the default label distribution protocol for the entire router or just for the PE-to-CE interface for VRF.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls label protocol ldp**
4. **interface** *type number*
5. **mpls label protocol ldp**
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config)# mpls label protocol ldp    | Specifies MPLS LDP as the default label distribution protocol for the router.                                                                                                                                                                                                                                          |
| Step 4 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0 | (Optional) Specifies the interface to configure and enters interface configuration mode.<br><ul style="list-style-type: none"><li>• The <i>type</i> argument specifies the type of interface to be configured.</li><li>• The <i>number</i> argument specifies the port, connector, or interface card number.</li></ul> |
| Step 5 | <b>mpls label protocol ldp</b><br><br><b>Example:</b><br>Router(config-if)# mpls label protocol ldp | (Optional) Specifies MPLS LDP as the default label distribution protocol for the interface.                                                                                                                                                                                                                            |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                              |

## Enabling MPLS Encapsulation on the CSC-PE and CSC-CE Routers

Every packet that crosses the backbone carrier must be encapsulated, so that the packet includes MPLS labels. You can enable MPLS encapsulation for the entire router or just on the interface of the PE or CE router. To enable the encapsulation of packets, perform the following task.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **interface** *type number*
5. **mpls ip**
6. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                |
|--------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                              | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                    |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                      |
| Step 3 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config)# mpls ip                                    | Enables MPLS encapsulation for the router.                                                                                                                                                                                                                                                                             |
| Step 4 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet5/0 | (Optional) Specifies the interface to configure and enters interface configuration mode.<br><ul style="list-style-type: none"><li>• The <i>type</i> argument specifies the type of interface to be configured.</li><li>• The <i>number</i> argument specifies the port, connector, or interface card number.</li></ul> |
| Step 5 | <b>mpls ip</b><br><br><b>Example:</b><br>Router(config-if)# mpls ip                                 | (Optional) Enables MPLS encapsulation for the specified interface.                                                                                                                                                                                                                                                     |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                       | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                              |

## Verifying the Carrier Supporting Carrier Configuration

The following commands verify the status of LDP sessions that were configured between the backbone carrier and customer carrier. Now the customer carrier ISP sites appear as a VPN customer to the backbone carrier.



## SUMMARY STEPS

1. `show mpls ldp discovery vrf vrf-name`
2. `show mpls ldp discovery all`

## DETAILED STEPS

### Step 1 `show mpls ldp discovery vrf vrf-name`

Use this command to show that the LDP sessions are in VRF VPN1 of the PE router of the backbone carrier, for example:

```
Router# show mpls ldp discovery vrf vpn1

Local LDP Identifier:
  10.0.0.0:0
Discovery Sources:
  Interfaces:
    Ethernet1/0 (ldp): xmit/recv
      LDP Id: 10.0.0.1:0
    POS6/0 (ldp): xmit
```

### Step 2 `show mpls ldp discovery all`

Use this command to list all LDP sessions in a router, for example:

```
Router# show mpls ldp discovery all

Local LDP Identifier:
  10.10.10.10:0
Discovery Sources:
  Interfaces:
    Ethernet1/5 (ldp): xmit/recv
      LDP Id: 10.5.5.5:0
VRF vpn1: Local LDP Identifier:
  10.0.0.1:0
Discovery Sources:
  Interfaces:
    Ethernet1/0 (ldp): xmit/recv
      LDP Id: 10.0.0.1:0
    POS6/0 (ldp): xmit
```

The Local LDP Identifier field shows the LDP identifier for the local label switching router for this session. The Interfaces field displays the interfaces engaging in LDP discovery activity:

- xmit indicates that the interface is transmitting LDP discovery hello packets.
- rcv indicates that the interface is receiving LDP discovery hello packets.

# Configuration Examples for MPLS VPN CSC with LDP and IGP

This section provides the following configuration examples:

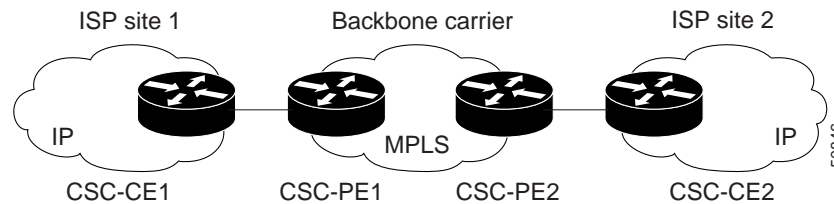
- [MPLS VPN CSC Network with a Customer Who Is an ISP: Example](#)
- [MPLS VPN CSC Network with a Customer Who Is an MPLS VPN Provider: Example](#)
- [MPLS VPN CSC Network That Contains Route Reflectors: Example](#)

- [MPLS VPN CSC Network with a Customer Who Has VPNs at the Network Edge: Example](#)

## MPLS VPN CSC Network with a Customer Who Is an ISP: Example

Figure 6 shows a carrier supporting carrier network configuration where the customer carrier is an ISP. The customer carrier has two sites, each of which is a POP. The customer carrier connects these sites using a VPN service provided by the backbone carrier. The backbone carrier uses MPLS. The ISP sites use IP. To enable packet transfer between the ISP sites and the backbone carrier, the CE routers that connect the ISPs to the backbone carrier run MPLS.

**Figure 6** *Carrier Supporting Carrier Network with a Customer Carrier Who Is an ISP*



The following examples show the configuration of each router in the carrier supporting carrier network. OSPF is used to connect the customer carrier to the backbone carrier.

### CSC-CE1 Configuration

```
mpls label protocol ldp
!
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 101 0 51 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
```

```

no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 10.14.14.14 0.0.0.0 area 200
network 10.15.0.0 0.255.255.255 area 200
network 10.16.0.0 0.255.255.255 area 200

```

## CSC-PE1 Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1

```

```

no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute bgp 100 metric-type 1 subnets
network 10.19.19.19 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.12.12.12 remote-as 100
neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-PE2 Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip directed-broadcast

```

```

no ip route-cache
no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.12.12.12 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.20.20.20 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.11.11.11 remote-as 100
 neighbor 10.11.11.11 update-source Loopback0
!

```

```
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family
```

## CSC-CE2 Configuration

```
ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
```

```

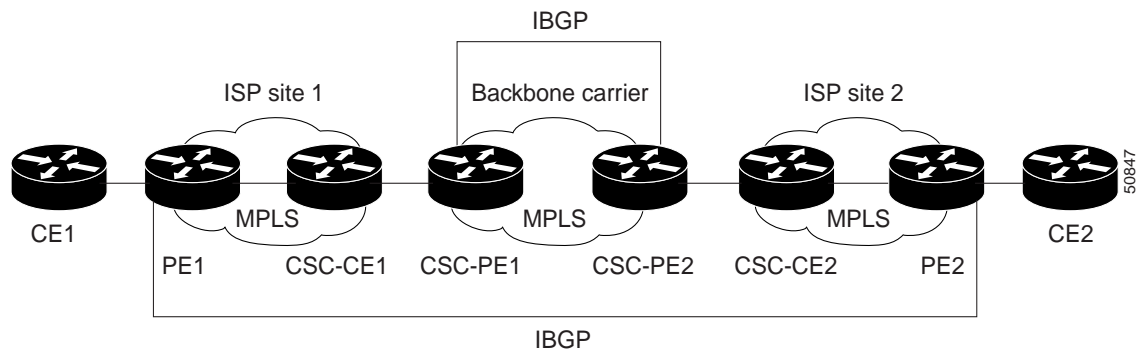
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.16.16.16 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
 network 10.0.0.0 0.255.255.255 area 200

```

## MPLS VPN CSC Network with a Customer Who Is an MPLS VPN Provider: Example

Figure 7 shows a carrier supporting carrier network configuration where the customer carrier is an MPLS VPN provider. The customer carrier has two sites. The backbone carrier and the customer carrier use MPLS. The IBGP sessions exchange the external routing information of the ISP.

**Figure 7** *Carrier Supporting Carrier Network with a Customer Carrier Who Is an MPLS VPN Provider*



The following configuration examples show the configuration of each router in the carrier supporting carrier network. OSPF is the protocol used to connect the customer carrier to the backbone carrier.

### CE1 Configuration

```

ip cef
!
interface Loopback0
 ip address 10.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 log-adjacency-changes
 redistribute bgp 300 subnets
 passive-interface Ethernet0/1
 network 10.17.17.17 0.0.0.0 area 300
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30

```

```
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.0.0.1 remote-as 200
neighbor 10.0.0.1 advertisement-interval 5
no auto-summary
```

## PE1 Configuration

```
ip cef
!
ip vrf vpn2
  rd 200:1
  route-target export 200:1
  route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
  ip address 10.13.13.13 255.255.255.255
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
!
interface ATM1/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  atm clock INTERNAL
  atm sonet stm-1
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  atm pvc 100 0 50 aal5snap
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls ip
!
interface Ethernet3/0
  ip vrf forwarding vpn2
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  no ip mroute-cache
!
router ospf 200
  log-adjacency-changes
  redistribute connected subnets
  passive-interface Ethernet3/0
  network 10.13.13.13 0.0.0.0 area 200
  network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor 10.15.15.15 remote-as 200
  neighbor 10.15.15.15 update-source Loopback0
  !
  address-family ipv4
    neighbor 10.15.15.15 activate
    neighbor 10.15.15.15 send-community extended
```



```

no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 as-override
neighbor 10.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE1 Configuration

```

mpls label protocol ldp
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200

```

```
log-adjacency-changes
redistribute connected subnets
network 10.14.14.14 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200
```

## CSC-PE1 Configuration

```
ip cef distributed
!
ip vrf vpn1
  rd 100:0
  route-target export 100:0
  route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
  ip address 11.11.11.11 255.255.255.255
  no ip directed-broadcast
  no ip route-cache
  no ip mroute-cache
!
interface Loopback100
  ip vrf forwarding vpn1
  ip address 10.19.19.19 255.255.255.255
  no ip directed-broadcast
!
interface ATM1/1/0
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  atm clock INTERNAL
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  atm pvc 100 0 50 aal5snap
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls ip
!
interface ATM3/0/0
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  atm clock INTERNAL
  atm sonet stm-1
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
  ip vrf forwarding vpn1
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  atm pvc 101 0 51 aal5snap
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls ip
!
```

```

router ospf 100
 log-adjacency-changes
 passive-interface ATM3/0/0.1
 passive-interface Loopback100
 network 10.11.11.11 0.0.0.0 area 100
 network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
 log-adjacency-changes
 redistribute bgp 100 metric-type 1 subnets
 network 10.19.19.19 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
!
 address-family ipv4
  neighbor 10.12.12.12 activate
  neighbor 10.12.12.12 send-community extended
 no synchronization
 exit-address-family
!
 address-family vpnv4
  neighbor 10.12.12.12 activate
  neighbor 10.12.12.12 send-community extended
 exit-address-family
!
 address-family ipv4 vrf vpn1
  redistribute ospf 200 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family

```

## CSC-PE2 Configuration

```

ip cef distributed
!
ip vrf vpn1
 rd 100:0
 route-target export 100:0
 route-target import 100:0
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Loopback100
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed

```

```
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.12.12.12 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute bgp 100 metric-type 1 subnets
network 10.20.20.20 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
```

```

redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 50 aal5snap
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 redistribute connected subnets
 network 10.16.16.16 0.0.0.0 area 200
 network 10.0.0.0 0.255.255.255 area 200
 network 10.0.0.0 0.255.255.255 area 200

```

## PE2 Configuration

```

ip cef

```

```
ip cef accounting non-recursive
!
ip vrf vpn2
  rd 200:1
  route-target export 200:1
  route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
  ip address 10.15.15.15 255.255.255.255
  no ip directed-broadcast
!
interface Ethernet3/0
  ip vrf forwarding vpn2
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
!
interface ATM5/0
  no ip address
  no ip directed-broadcast
  atm clock INTERNAL
  atm sonet stm-1
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
  ip address 10.0.0.1 255.0.0.0
  no ip directed-broadcast
  atm pvc 100 0 50 aal5snap
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls ip
!
router ospf 200
  log-adjacency-changes
  redistribute connected subnets
  passive-interface Ethernet3/0
  network 10.15.15.15 0.0.0.0 area 200
  network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor 10.13.13.13 remote-as 200
  neighbor 10.13.13.13 update-source Loopback0
  !
  address-family ipv4
    neighbor 10.13.13.13 activate
    neighbor 10.13.13.13 send-community extended
    no synchronization
    exit-address-family
  !
  address-family vpnv4
    neighbor 10.13.13.13 activate
    neighbor 10.13.13.13 send-community extended
    exit-address-family
  !
  address-family ipv4 vrf vpn2
    neighbor 10.0.0.2 remote-as 300
    neighbor 10.0.0.2 activate
    neighbor 10.0.0.2 as-override
    neighbor 10.0.0.2 advertisement-interval 5
    no auto-summary
```

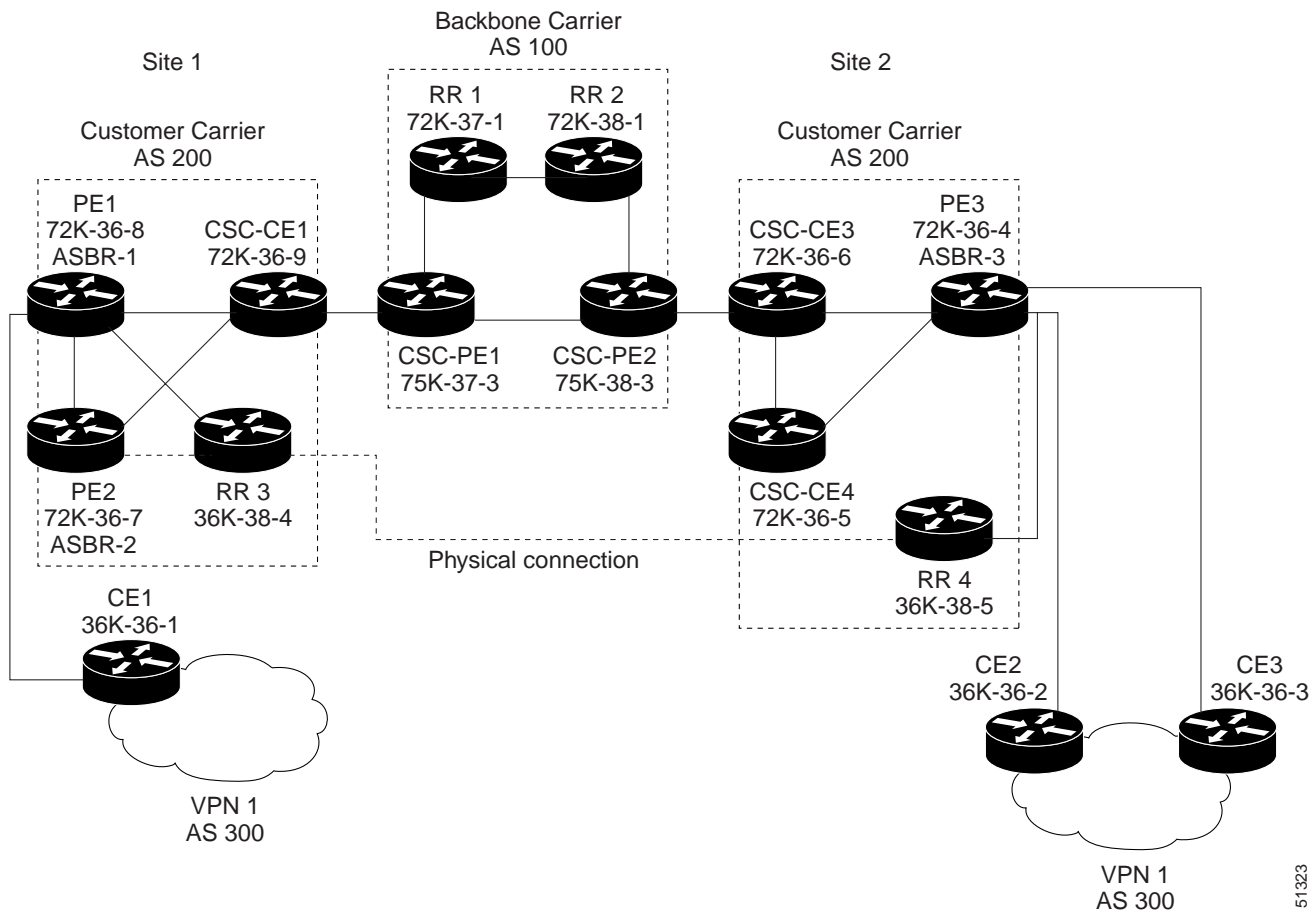
```
no synchronization
exit-address-family
```

## CE2 Configuration

```
ip cef
!
interface Loopback0
 ip address 10.18.18.18 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 log-adjacency-changes
 redistribute bgp 300 subnets
 passive-interface Ethernet0/1
 network 10.18.18.18 0.0.0.0 area 300
!
router bgp 300
 no synchronization
 bgp log-neighbor-changes
 timers bgp 10 30
 redistribute connected
 redistribute ospf 300 match internal external 1 external 2
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 advertisement-interval 5
 no auto-summary
```

## MPLS VPN CSC Network That Contains Route Reflectors: Example

Figure 8 shows a carrier supporting carrier network configuration that contains route reflectors. The customer carrier has two sites.

**Figure 8** Carrier Supporting Carrier Network that Contains Route Reflectors**Note**

A connection between route reflectors (RRs) is not necessary.

The following configuration examples show the configuration of each router in the carrier supporting carrier network. Note the following:

- The router IP addresses are abbreviated for ease of reading. For example, the loopback address for PE 1 is 25, which is equivalent to 10.25.25.25.
- The following list shows the loopback addresses for the CSC-PE routers:
  - CSC-PE1 (75K-37-3): loopback 0 = 10.15.15.15, loopback 1 = 10.18.18.18
  - CSC-PE2 (75K-38-3): loopback 0 = 10.16.16.16, loopback 1 = 10.20.20.20

## Backbone Carrier Configuration

### Route Reflector 1 (72K-37-1) Configuration

```
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
```



```

!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0.0 0.255.255.255 area 100
 network 10.2.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 10.15.15.15 remote-as 100
 neighbor 10.15.15.15 update-source Loopback0
 neighbor 10.16.16.16 remote-as 100
 neighbor 10.16.16.16 update-source Loopback0
!
 address-family ipv4 vrf vpn1
 no auto-summary
 no synchronization
 exit-address-family
!
 address-family vpnv4
 neighbor 10.15.15.15 activate
 neighbor 10.15.15.15 route-reflector-client
 neighbor 10.15.15.15 send-community extended
 neighbor 10.16.16.16 activate
 neighbor 10.16.16.16 route-reflector-client
 neighbor 10.16.16.16 send-community extended
 bgp scan-time import 5
 exit-address-family

```

## Route Reflector 2 (72K-38-1) Configuration

```
interface Loopback0
 ip address 10.14.14.14 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/0.1 mpls
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM1/1
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM1/1.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
router ospf 100
 auto-cost reference-bandwidth 10000
 network 10.0.0.0 0.255.255.255 area 100
 network 10.1.0 0.255.255.255 area 100
 network 10.2.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 1
 redistribute static
 neighbor 10.15.15.15 remote-as 100
 neighbor 10.15.15.15 update-source Loopback0
 neighbor 10.16.16.16 remote-as 100
 neighbor 10.16.16.16 update-source Loopback0
!
```

```

address-family ipv4 vrf vpn1
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 route-reflector-client
neighbor 10.15.15.15 send-community extended
neighbor 10.16.16.16 activate
neighbor 10.16.16.16 route-reflector-client
neighbor 10.16.16.16 send-community extended
bgp scan-time import 5
exit-address-family

```

### CSC-PE1 (75K-37-3) Configuration

```

ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
!
interface Loopback0
ip address 10.15.15.15 255.255.255.255
no ip directed-broadcast
!
interface Loopback1
ip vrf forwarding vpn1
ip address 10.18.18.18 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/0/1
ip vrf forwarding vpn1
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
no ip route-cache distributed
mpls label protocol ldp
mpls ip
!
interface ATM1/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 mpls
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL

```

```
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 6 32 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 mpls
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
no atm enable-ilmi-trap
mpls label protocol ldp
mpls atm vpi 2-5
mpls ip
!
router ospf 100
auto-cost reference-bandwidth 10000
network 10.0.0.0 0.255.255.255 area 100
network 10.1.0.0 0.255.255.255 area 100
network 10.2.0.0 0.255.255.255 area 100
network 10.3.0.0 0.255.255.255 area 100
network 10.4.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
redistribute bgp 100 metric-type 1 subnets
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 10.13.13.13 remote-as 100
neighbor 10.13.13.13 update-source Loopback0
neighbor 10.14.14.14 remote-as 100
neighbor 10.14.14.14 update-source Loopback0
!
address-family ipv4
redistribute static
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
exit-address-family
```

```

!
address-family ipv4 vrf vpn1
 redistribute ospf 1 match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family

```

### CSC-PE2 (75K-38-3) Configuration

```

ip cef distributed
!
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
interface Loopback0
 ip address 10.16.16.16 255.255.255.255
 no ip directed-broadcast
!
interface Loopback1
 ip vrf forwarding vpn1
 ip address 10.20.20.20 255.255.255.255
 no ip directed-broadcast
!
interface ATM0/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM2/1/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM2/1/0.1 mpls
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 mpls label protocol ldp
 mpls atm vpi 2-5
 mpls ip
!
interface ATM3/0/0
 no ip address
 no ip directed-broadcast
 no ip route-cache distributed

```

```
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 100 6 32 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
atm pvc 101 6 33 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
auto-cost reference-bandwidth 10000
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 1 vrf vpn1
redistribute bgp 100 metric-type 1 subnets
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
network 10.0.0.0 0.255.255.255 area 101
!
router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 10.13.13.13 remote-as 100
neighbor 10.13.13.13 update-source Loopback0
neighbor 10.14.14.14 remote-as 100
neighbor 10.14.14.14 update-source Loopback0
!
address-family ipv4
redistribute static
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
```

```

neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 1 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## Customer Carrier Site 1 Configuration

### PE1 (72K-36-8) Configuration

```

ip cef
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
ip address 10.25.25.25 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0
ip vrf forwarding vpn2
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet3/1
ip address 10.0.0.1 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/2
ip address 10.0.0.2 255.0.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!

```

```

router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
!
 address-family ipv4 vrf vpn2
  redistribute connected
  neighbor 10.0.0.2 remote-as 300
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 as-override
  no auto-summary
  no synchronization
  exit-address-family
!
 address-family vpnv4
  neighbor 10.22.22.22 activate
  neighbor 10.22.22.22 send-community extended
  neighbor 10.23.23.23 activate
  neighbor 10.23.23.23 send-community extended
  exit-address-family

```

### CSC-CE1 (72K-36-9) Configuration

```

ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 10.11.11.11 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast

```



```

    atm pvc 100 0 50 aal5snap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101

```

## PE2 (72K-36-7) Configuration

```

ip cef
!
ip vrf vpn2
 rd 200:1
  route-target export 200:1
  route-target import 200:1
no mpls ip propagate-ttl
!
interface Loopback0
 ip address 10.24.24.24 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface Ethernet3/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet3/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
mpls label protocol ldp
mpls ip
!

```

```

interface Ethernet3/3
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
 network 10.0.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
!
 address-family ipv4 vrf vpn2
  neighbor 10.0.0.2 remote-as 300
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.2 as-override
  no auto-summary
  no synchronization
 exit-address-family
!
 address-family vpnv4
  neighbor 10.22.22.22 activate
  neighbor 10.22.22.22 send-community extended
  neighbor 10.23.23.23 activate
  neighbor 10.23.23.23 send-community extended
 exit-address-family

```

### Route Reflector 3 (36K-38-4) Configuration

```

ip cef
!
interface Loopback0
 ip address 10.23.23.23 255.255.255.255
!
interface Ethernet1/1
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface Ethernet1/2
 ip address 10.0.0.1 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface ATM3/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM3/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip

```

```

!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 10.21.21.21 remote-as 200
 neighbor 10.21.21.21 update-source Loopback0
 neighbor 10.24.24.24 remote-as 200
 neighbor 10.24.24.24 update-source Loopback0
 neighbor 10.25.25.25 remote-as 200
 neighbor 10.25.25.25 update-source Loopback0
!
 address-family ipv4 vrf vpn2
  no auto-summary
  no synchronization
 exit-address-family
!
 address-family vpnv4
  neighbor 10.21.21.21 activate
  neighbor 10.21.21.21 route-reflector-client
  neighbor 10.21.21.21 send-community extended
  neighbor 10.24.24.24 activate
  neighbor 10.24.24.24 route-reflector-client
  neighbor 10.24.24.24 send-community extended
  neighbor 10.25.25.25 activate
  neighbor 10.25.25.25 route-reflector-client
  neighbor 10.25.25.25 send-community extended
 exit-address-family

```

## CE1 (36K-36-1) Configuration

```

ip cef
!
interface Loopback0
 ip address 10.28.28.28 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet0/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router bgp 300
 network 10.0.0.0
 network 10.0.0.0
 network 10.0.0.0
 neighbor 10.0.0.1 remote-as 200
 neighbor 10.0.0.1 remote-as 200

```

## Customer Carrier Site 2 Configuration

### CSC-CE3 (72K-36-6) Configuration

```

ip cef
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
!
interface ATM1/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 32 aal5snap
 mpls label protocol ldp

 mpls ip
!
interface POS2/0
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
 mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101

```

### PE3 (72K-36-4) Configuration

```

ip cef
!
ip vrf vpn2
 rd 200:1
 route-target export 200:1
 route-target import 200:1
!

```

```

!
interface Loopback0
 ip address 10.21.21.21 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet3/0
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/1
 ip vrf forwarding vpn2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet3/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
mpls label protocol ldp
mpls ip
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 40 aal5snap
mpls label protocol ldp
mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
mpls label protocol ldp
mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101
!
router bgp 200
 neighbor 10.22.22.22 remote-as 200
 neighbor 10.22.22.22 update-source Loopback0
 neighbor 10.23.23.23 remote-as 200
 neighbor 10.23.23.23 update-source Loopback0
!
 address-family ipv4 vrf vpn2
  redistribute connected
 neighbor 10.0.0.2 remote-as 300
 neighbor 10.0.0.2 activate
 neighbor 10.0.0.2 as-override

```

```

neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.22.22.22 activate
neighbor 10.22.22.22 send-community extended
neighbor 10.23.23.23 activate
neighbor 10.23.23.23 send-community extended
exit-address-family

```

### CSC-CE4 (72K-36-5) Configuration

```

ip cef
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
 no ip directed-broadcast
!
interface POS4/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
  clock source internal
!
interface ATM5/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 0 20 aal5snap
 mpls label protocol ldp
 mpls ip
!
interface ATM6/0
 no ip address
 no ip directed-broadcast
 atm clock INTERNAL
 no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
 atm pvc 100 6 33 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
 network 10.3.0.0 0.255.255.255 area 101

```

**Route Reflector 4 (36K-38-5) Configuration**

```

ip cef
!
interface Loopback0
 ip address 10.22.22.22 255.255.255.255
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 mpls label protocol ldp
 mpls ip
!
interface ATM2/0
 no ip address
 no ip mroute-cache
 atm clock INTERNAL
 no atm scrambling cell-payload
 no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
 ip address 10.0.0.1 255.0.0.0
 atm pvc 100 0 55 aal5snap
 mpls label protocol ldp
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 101
 network 10.1.0.0 0.255.255.255 area 101
 network 10.2.0.0 0.255.255.255 area 101
!
router bgp 200
 no synchronization
 no bgp default ipv4-unicast
 bgp cluster-id 2
 redistribute static
 neighbor 10.21.21.21 remote-as 200
 neighbor 10.21.21.21 update-source Loopback0
 neighbor 10.24.24.24 remote-as 200
 neighbor 10.24.24.24 update-source Loopback0
 neighbor 10.25.25.25 remote-as 200
 neighbor 10.25.25.25 update-source Loopback0
!
 address-family ipv4 vrf vpn2
  no auto-summary
  no synchronization
  exit-address-family
!
 address-family vpnv4
  neighbor 10.21.21.21 activate
  neighbor 10.21.21.21 route-reflector-client
  neighbor 10.21.21.21 send-community extended
  neighbor 10.24.24.24 activate
  neighbor 10.24.24.24 route-reflector-client
  neighbor 10.24.24.24 send-community extended
  neighbor 10.25.25.25 activate
  neighbor 10.25.25.25 route-reflector-client
  neighbor 10.25.25.25 send-community extended
  exit-address-family

```

### CE2 (36K-36-2) Configuration

```
ip cef
!
interface Loopback0
 ip address 10.26.26.26 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet0/2
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 10.0.0.0 0.255.255.255 area 300
 network 10.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 10.0.0.0
 network 10.1.0.0
 network 10.2.0.0
 neighbor 10.0.0.1 remote-as 200
```

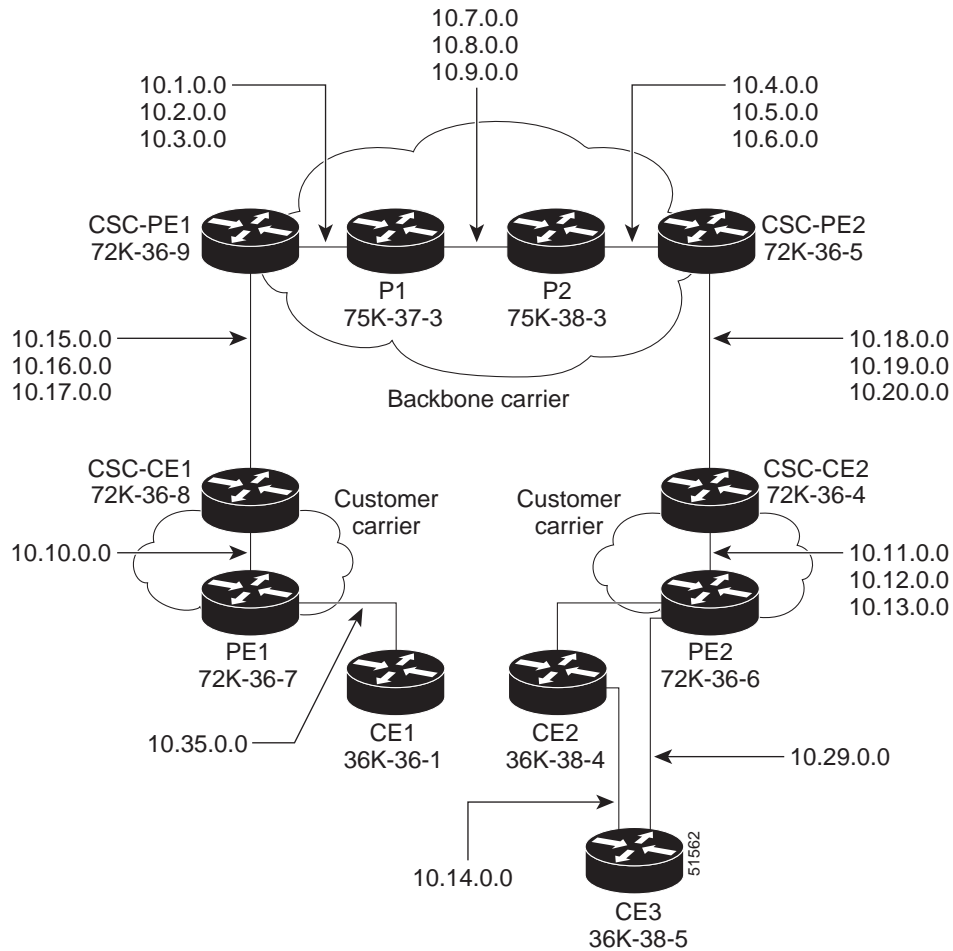
### CE3 (36K-36-3) Configuration

```
ip cef
!
interface Loopback0
 ip address 10.27.27.27 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet1/1
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
interface Ethernet1/2
 ip address 10.0.0.2 255.0.0.0
 no ip directed-broadcast
!
router ospf 300
 redistribute bgp 300
 network 10.0.0.0 0.255.255.255 area 300
 network 10.0.0.0 0.255.255.255 area 300
!
router bgp 300
 network 10.0.0.0
 network 10.1.0.0
 network 10.2.0.0
 neighbor 10.0.0.1 remote-as 200
```

## MPLS VPN CSC Network with a Customer Who Has VPNs at the Network Edge: Example

Figure 9 shows a carrier supporting carrier network configuration where the customer carrier has VPNs at the network edge.



**Figure 9** *Carrier Supporting Carrier Network*

## Backbone Carrier Configuration

### CSC-PE1 (72K-36-9) Configuration

```

ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
!
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1

```

```
ip address 10.22.22.22 255.255.255.255
no ip directed-broadcast
!
interface ATM1/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.1.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 10.2.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 10.3.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM2/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.15.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0.2 point-to-point
ip vrf forwarding vpn1
ip address 10.16.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM2/0.3 point-to-point
ip vrf forwarding vpn1
ip address 10.17.0.2 255.255.0.0
```

```

no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM2/0.1
passive-interface ATM2/0.2
passive-interface ATM2/0.3
passive-interface Loopback100
network 10.14.14.14 0.0.0.0 area 100
network 10.1.0.0 0.0.255.255 area 100
network 10.2.0.0 0.0.255.255 area 100
network 10.3.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 10.22.22.22 0.0.0.0 area 200
network 10.15.0.0 0.0.255.255 area 200
network 10.16.0.0 0.0.255.255 area 200
network 10.17.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## P1 (75K-37-3) Configuration

```

ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/1/0

```

```
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/1/0.1 point-to-point
ip address 10.7.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.2 point-to-point
ip address 10.8.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/1/0.3 point-to-point
ip address 10.9.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/0/0.1 point-to-point
ip address 10.1.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls accounting experimental input
tag-switching ip
!
interface ATM3/0/0.2 point-to-point
ip address 10.2.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/0/0.3 point-to-point
ip address 10.3.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
```

```

!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 10.12.12.12 0.0.0.0 area 100
network 10.1.0.0 0.0.255.255 area 100
network 10.2.0.0 0.0.255.255 area 100
network 10.3.0.0 0.0.255.255 area 100
network 10.7.0.0 0.0.255.255 area 100
network 10.8.0.0 0.0.255.255 area 100
network 10.9.0.0 0.0.255.255 area 100

```

## P2 (75K-38-3) Configuration

```

ip cef distributed
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.13.13.13 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM0/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM0/1/0.1 point-to-point
ip address 10.7.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 103 0 53 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM0/1/0.2 point-to-point
ip address 10.8.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 104 0 54 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM0/1/0.3 point-to-point
ip address 10.9.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 105 0 55 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0
no ip address
no ip directed-broadcast
ip route-cache distributed
atm clock INTERNAL
atm sonet stm-1

```

```

no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM3/1/0.1 point-to-point
ip address 10.4.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0.2 point-to-point
ip address 10.5.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM3/1/0.3 point-to-point
ip address 10.6.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
network 10.13.13.13 0.0.0.0 area 100
network 10.4.0.0 0.0.255.255 area 100
network 10.5.0.0 0.0.255.255 area 100
network 10.6.0.0 0.0.255.255 area 100
network 10.7.0.0 0.0.255.255 area 100
network 10.8.0.0 0.0.255.255 area 100
network 10.9.0.0 0.0.255.255 area 100
!

```

### CSC-PE2 (72K-36-5) Configuration

```

ip cef
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.23.23.23 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast

```

```

no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.18.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip vrf forwarding vpn1
ip address 10.19.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip vrf forwarding vpn1
ip address 10.20.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 10.4.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.2 point-to-point
ip address 10.5.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 10.6.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp

```

```

tag-switching ip
!
router ospf 100
log-adjacency-changes
redistribute connected subnets
passive-interface ATM5/0.1
passive-interface ATM5/0.2
passive-interface ATM5/0.3
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.4.0.0 0.0.255.255 area 100
network 10.5.0.0 0.0.255.255 area 100
network 10.6.0.0 0.0.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
redistribute connected subnets
redistribute bgp 100 metric-type 1 subnets
network 10.23.23.23 0.0.0.0 area 200
network 10.18.0.0 0.0.255.255 area 200
network 10.19.0.0 0.0.255.255 area 200
network 10.20.0.0 0.0.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.14.14.14 remote-as 100
neighbor 10.14.14.14 update-source Loopback0
!
address-family ipv4
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## Customer Carrier Site 1 Configuration

### CSC-CE1 (72K-36-8) Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.15.15.15 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address

```



```

no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
ip address 10.15.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.2 point-to-point
ip address 10.16.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM1/0.3 point-to-point
ip address 10.17.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface Ethernet3/1
ip address 10.10.0.2 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 10.15.15.15 0.0.0.0 area 200
network 10.10.0.0 0.0.255.255 area 200
network 10.15.0.0 0.0.255.255 area 200
network 10.16.0.0 0.0.255.255 area 200
network 10.17.0.0 0.0.255.255 area 200

```

## PE1 (72K-36-7) Configuration

```

ip cef
!
ip vrf customersite
rd 200:1
route-target export 200:1
route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!

```

```

interface Ethernet3/1
ip vrf forwarding customersite
ip address 10.35.0.2 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
!
interface Ethernet3/2
ip address 30.10.0.1 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
passive-interface Ethernet3/1
network 10.16.16.16 0.0.0.0 area 200
network 10.10.0.0 0.0.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.18.18.18 remote-as 200
neighbor 10.18.18.18 update-source Loopback0
!
address-family ipv4
neighbor 10.18.18.18 activate
neighbor 10.18.18.18 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.18.18.18 activate
neighbor 10.18.18.18 send-community extended
exit-address-family
!
address-family ipv4 vrf customersite
neighbor 10.35.0.1 remote-as 300
neighbor 10.35.0.1 activate
neighbor 10.35.0.1 as-override
neighbor 10.35.0.1 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

### CE1 (36K-36-1) Configuration

```

ip cef
!
interface Loopback0
ip address 10.19.19.19 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 30.35.0.1 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets

```

```

passive-interface Ethernet0/2
network 10.19.19.19 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.35.0.2 remote-as 200
neighbor 10.35.0.2 advertisement-interval 5
no auto-summary

```

## Customer Carrier Site 2 Configuration

### CSC-CE2 (72K-36-4) Configuration

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
ip address 10.17.17.17 255.255.255.255
no ip directed-broadcast
!
interface ATM5/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 10.11.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip address 10.12.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 10.13.0.2 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
atm sonet stm-1

```

```

no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM6/0.1 point-to-point
ip address 10.18.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.2 point-to-point
ip address 10.19.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM6/0.3 point-to-point
ip address 10.20.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
network 10.17.17.17 0.0.0.0 area 200
network 10.11.0.0 0.0.255.255 area 200
network 10.12.0.0 0.0.255.255 area 200
network 10.13.0.0 0.0.255.255 area 200
network 10.18.0.0 0.0.255.255 area 200
network 10.19.0.0 0.0.255.255 area 200
network 10.20.0.0 0.0.255.255 area 200

```

## PE2 (72K-36-6) Configuration

```

ip cef
!
ip vrf customersite
rd 200:1
route-target export 200:1
route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
ip address 10.18.18.18 255.255.255.255
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
!
interface Ethernet3/0
ip vrf forwarding customersite
ip address 10.29.0.2 255.255.0.0
no ip directed-broadcast
!
interface Ethernet3/1
ip vrf forwarding customersite
ip address 10.30.0.2 255.255.0.0
no ip directed-broadcast

```

```

!
interface ATM5/0
no ip address
no ip directed-broadcast
no ip mroute-cache
atm clock INTERNAL
atm sonet stm-1
no atm enable-ilmi-trap
no atm ilmi-keepalive
!
interface ATM5/0.1 point-to-point
ip address 10.11.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.2 point-to-point
ip address 10.12.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
interface ATM5/0.3 point-to-point
ip address 10.13.0.1 255.255.0.0
no ip directed-broadcast
atm pvc 102 0 52 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
tag-switching ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
passive-interface Ethernet3/0
passive-interface Ethernet3/1
network 10.18.18.18 0.0.0.0 area 200
network 10.11.0.0 0.0.255.255 area 200
network 10.12.0.0 0.0.255.255 area 200
network 10.13.0.0 0.0.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor 10.16.16.16 remote-as 200
neighbor 10.16.16.16 update-source Loopback0
!
address-family ipv4
neighbor 10.16.16.16 activate
neighbor 10.16.16.16 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.16.16.16 activate
neighbor 10.16.16.16 send-community extended
exit-address-family
!
address-family ipv4 vrf customersite
neighbor 10.29.0.1 remote-as 300

```

```
neighbor 10.29.0.1 activate
neighbor 10.29.0.1 as-override
neighbor 10.29.0.1 advertisement-interval 5
neighbor 10.30.0.1 remote-as 300
neighbor 10.30.0.1 activate
neighbor 10.30.0.1 as-override
neighbor 10.30.0.1 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

### CE2 (36K-38-4) Configuration

```
ip cef
!
interface Loopback0
ip address 10.21.21.21 255.255.255.255
!
interface Ethernet1/3
ip address 10.29.0.1 255.255.0.0
!
interface Ethernet5/0
ip address 10.14.0.1 255.255.0.0
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet1/3
network 10.21.21.21 0.0.0.0 area 300
network 10.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.29.0.2 remote-as 200
neighbor 10.29.0.2 advertisement-interval 5
no auto-summary
```

### CE3 (36K-38-5) Configuration

```
ip cef
!
interface Loopback0
ip address 10.20.20.20 255.255.255.255
no ip directed-broadcast
!
interface Ethernet0/2
ip address 10.30.0.1 255.255.0.0
no ip directed-broadcast
!
interface Ethernet0/3
ip address 10.14.0.2 255.255.0.0
no ip directed-broadcast
!
router ospf 300
log-adjacency-changes
redistribute connected subnets
redistribute bgp 300 subnets
passive-interface Ethernet0/2
network 10.20.20.20 0.0.0.0 area 300
```

```

network 10.14.0.0 0.0.255.255 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.30.0.2 remote-as 200
neighbor 10.30.0.2 advertisement-interval 5
no auto-summary

```

## Additional References

The following sections provide references related to MPLS VPNs.

### Related Documents

| Related Topic | Document Title                          |
|---------------|-----------------------------------------|
| MPLS          | <a href="#">MPLS Product Literature</a> |

### Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title         |
|----------|---------------|
| RFC 2547 | BGP/MPLS VPNs |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

This feature uses no new or modified commands.



# Feature Information for MPLS VPN CSC with LDP and IGP

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 4** Feature Information for MPLS VPN CSC with LDP and IGP

| Feature Name                        | Releases                                                                     | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN Carrier Supporting Carrier | 12.0(14)ST<br>12.0(16)ST<br>12.2(8)T<br>12.0(21)ST<br>12.0(22)S<br>12.0(23)S | This feature enables you to set up and create an MPLS VPN CSC network that uses LDP to transport MPLS labels and an IGP to transport routes.<br><br>In 12.0(14)ST, this feature was introduced.<br>In 12.0(16)ST, this feature was integrated.<br>In 12.2(8)T, this feature was integrated.<br>In 12.0(21)ST, this feature was integrated.<br>In 12.0(22)S, this feature was integrated.<br>In 12.0(23)S, this feature was integrated. |

## Glossary

**ASBR**—autonomous system boundary router. A router that connects one autonomous system to another.

**BGP**—Border Gateway Protocol. An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

**carrier supporting carrier**—A situation where one service provider allows another service provider to use a segment of its backbone network.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. In this document, the CE router sits on the edge of the customer carrier network.

**edge router**—A router that is at the edge of the network. It defines the boundary of the MPLS network. It receives and transmits packets. Also referred to as edge label switch router and label edge router.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**PE router**—provider edge router. A router, at the edge of a service provider's network, that interfaces to CE routers.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

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

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

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

© 2005—2009 Cisco Systems, Inc. All rights reserved.





# MPLS VPN Carrier Supporting Carrier with BGP

---

**First Published: May 2, 2005**

**Last Updated: February 5, 2009**

Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) Carrier Supporting Carrier (CSC) enables one MPLS VPN-based service provider to allow other service providers to use a segment of its backbone network. This module explains how to configure an MPLS VPN CSC network that uses Border Gateway Protocol (BGP) to distribute routes and MPLS labels.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS VPN CSC with BGP”](#) section on page 50.

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

## Contents

- [Prerequisites for MPLS VPN CSC with BGP, page 2](#)
- [Restrictions for MPLS VPN CSC with BGP, page 2](#)
- [Information About MPLS VPN CSC with BGP, page 2](#)
- [How to Configure MPLS VPN CSC with BGP, page 5](#)
- [Configuration Examples for MPLS VPN CSC with BGP, page 32](#)
- [Additional References, page 47](#)
- [Command Reference, page 49](#)
- [Feature Information for MPLS VPN CSC with BGP, page 50](#)
- [Glossary, page 51](#)



---

**Americas Headquarters:**

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

## Prerequisites for MPLS VPN CSC with BGP

- You should be able to configure MPLS VPNs with end-to-end (CE-to-CE router) pings working. To accomplish this, you need to know how to configure Interior Gateway Protocols (IGPs), MPLS Label Distribution Protocol (LDP), and Multiprotocol Border Gateway Protocol (MP-BGP).
- Make sure that the CSC-PE routers and the CSC-CE routers run images that support BGP label distribution. Otherwise, you cannot run external BGP (EBGP) between them. Ensure that connectivity between the customer carrier and the backbone carrier. EBGP-based label distribution is configured on these links to enable MPLS between the customer and backbone carriers.

## Restrictions for MPLS VPN CSC with BGP

On a provider edge (PE) router, you can configure an interface for either BGP with labels or LDP. You cannot enable both types of label distribution on the same interface. If you switch from one protocol to the other, then you must disable the existing protocol on all interfaces before enabling the other protocol.

This feature does not support the following:

- EBGP multihop between CSC-PE and CSC-CE routers
- EIBGP multipath load sharing

The physical interfaces that connect the BGP speakers must support Cisco Express Forwarding or distributed Cisco Express Forwarding and MPLS.

## Information About MPLS VPN CSC with BGP

Before configuring MPLS VPN CSC, you should understand the following concepts:

- [MPLS VPN CSC Introduction, page 2](#)
- [Benefits of Implementing MPLS VPN CSC, page 3](#)
- [Benefits of Implementing MPLS VPN CSC with BGP, page 3](#)
- [Configuration Options for MPLS VPN CSC with BGP, page 4](#)

## MPLS VPN CSC Introduction

Carrier supporting carrier is where one service provider allows another service provider to use a segment of its backbone network. The service provider that provides the segment of the backbone network to the other provider is called the backbone carrier. The service provider that uses the segment of the backbone network is called the customer carrier.

A backbone carrier offers Border Gateway Protocol and Multiprotocol Label Switching (BGP/MPLS) VPN services. The customer carrier can be either:

- An Internet service provider (ISP)
- A BGP/MPLS VPN service provider

## Benefits of Implementing MPLS VPN CSC

The MPLS VPN CSC network provides the following benefits to service providers who are backbone carriers and to customer carriers.

### Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone. The backbone carrier does not need to create and maintain separate backbones for its customer carriers. Using one backbone network to support multiple customer carriers simplifies the backbone carrier's VPN operations. The backbone carrier uses a consistent method for managing and maintaining the backbone network. This is also cheaper and more efficient than maintaining separate backbones.
- The MPLS VPN carrier supporting carrier feature is scalable. Carrier supporting carrier can change the VPN to meet changing bandwidth and connectivity needs. The feature can accommodate unplanned growth and changes. The carrier supporting carrier feature enables tens of thousands of VPNs to be set up over the same network, and it allows a service provider to offer both VPN and Internet services.
- The MPLS VPN carrier supporting carrier feature is a flexible solution. The backbone carrier can accommodate many types of customer carriers. The backbone carrier can accept customer carriers who are ISPs or VPN service providers or both. The backbone carrier can accommodate customer carriers that require security and various bandwidths.

### Benefits to the Customer Carriers

- The MPLS VPN carrier supporting carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone. The customer carrier uses the backbone network of a backbone carrier, but the backbone carrier is responsible for network maintenance and operation.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide. Customer carriers can also use IPSec in their VPNs for a higher level of security; it is completely transparent to the backbone carrier.
- Customer carriers can use any link layer technology (SONET, DSL, Frame Relay, and so on) to connect the CE routers to the PE routers and the PE routers to the P routers. The MPLS VPN carrier supporting carrier feature is link layer independent. The CE routers and PE routers use IP to communicate, and the backbone carrier uses MPLS.
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier. The customer address space and routing information are independent of the address space and routing information of other customer carriers or the backbone provider.

## Benefits of Implementing MPLS VPN CSC with BGP

You can configure your CSC network to enable BGP to transport routes and MPLS labels between the backbone carrier PE routers and the customer carrier CE routers using multiple paths. The benefits of using BGP to distribute IPv4 routes and MPLS label routes are:

- BGP takes the place of an IGP and LDP in a VPN forwarding/routing instance (VRF) table. You can use BGP to distribute routes and MPLS labels. Using a single protocol instead of two simplifies the configuration and troubleshooting.

- BGP is the preferred routing protocol for connecting two ISPs, mainly because of its routing policies and ability to scale. ISPs commonly use BGP between two providers. This feature enables those ISPs to use BGP.

## Configuration Options for MPLS VPN CSC with BGP

The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be either of the following:

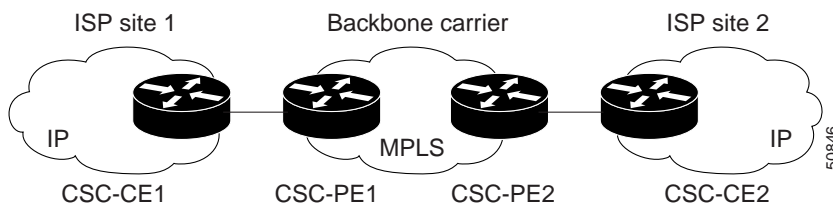
- [Customer Carrier Is an ISP with an IP Core, page 4](#)
- [Customer Carrier Is an MPLS Service Provider With or Without VPN Services, page 4](#)

The following sections explain how the backbone and customer carriers distribute IPv4 routes and MPLS labels.

### Customer Carrier Is an ISP with an IP Core

[Figure 1](#) shows a network configuration where the customer carrier is an ISP. The customer carrier has two sites, each of which is a point of presence (POP). The customer carrier connects these sites using a VPN service provided by the backbone carrier. The backbone carrier uses MPLS. The ISP sites use IP.

**Figure 1** Network Where the Customer Carrier Is an ISP



The links between the CE and PE routers use EBGp to distribute IPv4 routes and MPLS labels. Between the links, the PE routers use multiprotocol IBGP to distribute VPNv4 routes.

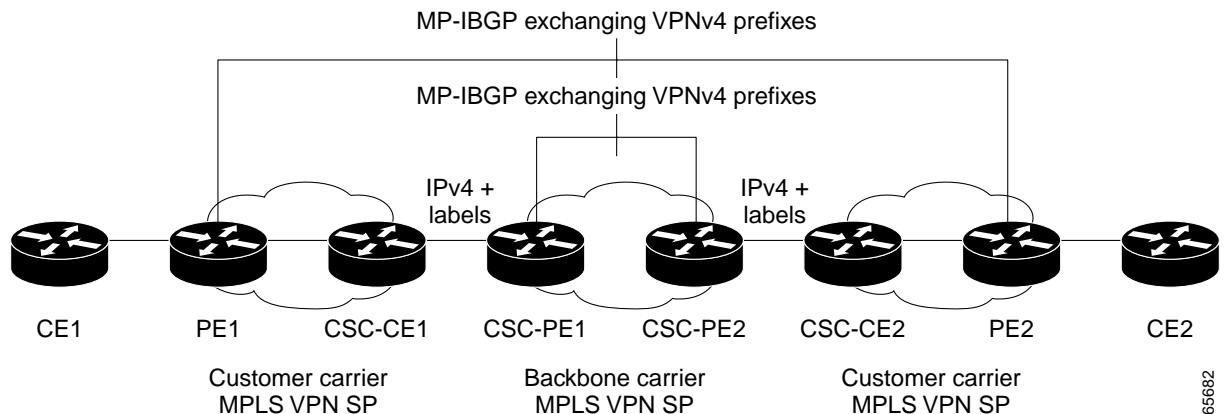


#### Note

If a router other than a Cisco router is used as a CSC-PE or CSC-CE, that router must support IPv4 BGP label distribution (RFC 3107). Otherwise, you cannot run EBGp with labels between the routers.

### Customer Carrier Is an MPLS Service Provider With or Without VPN Services

[Figure 2](#) shows a network configuration where the backbone carrier and the customer carrier are BGP/MPLS VPN service providers. This is known as hierarchical VPNs. The customer carrier has two sites. Both the backbone carrier and the customer carrier use MPLS in their networks.

**Figure 2** Network Where the Customer Carrier Is an MPLS VPN Service Provider

In this configuration, the customer carrier can configure its network in one of the following ways:

- The customer carrier can run IGP and LDP in its core network. In this case, the CSC-CE1 router in the customer carrier redistributes the EBGP routes it learns from the CSC-PE1 router of the backbone carrier to IGP.
- The CSC-CE1 router of the customer carrier system can run an IPv4 and labels IBGP session with the PE1 router.

## How to Configure MPLS VPN CSC with BGP

This section contains the following tasks:

- [Identifying the Carrier Supporting Carrier Topology, page 5](#) (required)
- [Configuring the Backbone Carrier Core, page 6](#) (required)
- [Configuring the CSC-PE and CSC-CE Routers, page 12](#) (required)
- [Configuring the Customer Carrier Network, page 21](#) (required)
- [Configuring the Customer Site for Hierarchical VPNs, page 24](#) (required)

## Identifying the Carrier Supporting Carrier Topology

Before you configure the MPLS VPN CSC with BGP, you need to identify both the backbone and customer carrier topology.

For hierarchical VPNs, the customer carrier of the MPLS VPN network provides MPLS VPN services to its own customers. In this instance, you need to identify the type of customer carrier as well as the topology of the customer carriers. Hierarchical VPNs require extra configuration steps, which are noted in the configuration sections.



### Note

You can connect multiple CSC-CE routers to the same PE, or you can connect a single CSC-CE router to CSC-PEs using more than one interface to provide redundancy and multiple path support in CSC topology.

Perform this task to identify the carrier supporting carrier topology.



## SUMMARY STEPS

1. Identify the type of customer carrier, ISP or MPLS VPN service provider.
2. (For hierarchical VPNs only) Identify the CE routers.
3. (For hierarchical VPNs only) Identify the customer carrier core router configuration.
4. Identify the customer carrier edge (CSC-CE) routers.
5. Identify backbone carrier router configuration.

## DETAILED STEPS

|        | Command or Action                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Identify the type of customer carrier, ISP or MPLS VPN service provider.              | Sets up requirements for configuration of carrier supporting carrier network. <ul style="list-style-type: none"> <li>• For an ISP, customer site configuration is not required.</li> <li>• For an MPLS VPN service provider, the customer site needs to be configured, as well as any task or step designated “for hierarchical VPNs only.”</li> </ul> |
| Step 2 | (For hierarchical VPNs only) Identify the CE routers.                                 | Sets up requirements for configuration of CE to PE connections.                                                                                                                                                                                                                                                                                        |
| Step 3 | (For hierarchical VPNs only) Identify the customer carrier core router configuration. | Sets up requirements for connection configuration between core (P) routers and between P routers and edge routers (PE and CSC-CE routers).                                                                                                                                                                                                             |
| Step 4 | Identify the customer carrier edge (CSC-CE) routers.                                  | Sets up requirements for configuration of CSC-CE to CSC-PE connections.                                                                                                                                                                                                                                                                                |
| Step 5 | Identify the backbone carrier router configuration.                                   | Sets up requirements for connection configuration between CSC core routers and between CSC core routers and edge routers (CSC-CE and CSC-PE routers).                                                                                                                                                                                                  |

## What to Do Next

Set up your carrier supporting carrier networks with the [“Configuring the Backbone Carrier Core” section on page 6](#).

## Configuring the Backbone Carrier Core

Configuring the backbone carrier core requires setting up connectivity and routing functions for the CSC core and the CSC-PE routers.

Configuring and verifying the CSC core (backbone carrier) involves the following tasks:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core, page 7](#) (optional)
- [Configuring VRFs for CSC-PE Routers, page 8](#) (required)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier, page 10](#) (required)

## Prerequisites

Before you configure a backbone carrier core, configure the following on the CSC core routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on.
- Label Distribution Protocol (LDP). For information, see [How to Configure MPLS LDP](#).

## Verifying IP Connectivity and LDP Configuration in the CSC Core

Perform this task to verify IP connectivity and LDP configuration in the CSC core.

### SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
5. **show mpls ldp discovery** [**vrf** *vrf-name* | **all**]
6. **show mpls ldp neighbor** [[**vrf** *vrf-name*] [*address* | *interface*] [**detail**] | **all**]
7. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
8. **show mpls interfaces** [[**vrf** *vrf-name*] [*interface*] [**detail**] | **all**]
9. **show ip route**
10. **disable**

### DETAILED STEPS

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                          | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                     |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system-address</i> }<br><br><b>Example:</b><br>Router# ping ip 10.1.0.0 | (Optional) Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks.<br><ul style="list-style-type: none"><li>• Use the <b>ping ip</b> command to verify the connectivity from one CSC core router to another.</li></ul>                                                                                             |
| Step 3 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip 10.2.0.0                     | (Optional) Discovers the routes that packets will actually take when traveling to their destination.<br><ul style="list-style-type: none"><li>• Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li></ul> |

|         | Command or Action                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4  | <pre>show mpls forwarding-table [vrf vrf-name] [{network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]]} [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table</p> | <p>(Optional) Displays the contents of the MPLS label forwarding information base (LFIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to verify that MPLS packets are being forwarded.</li> </ul>                         |
| Step 5  | <pre>show mpls ldp discovery [vrf vrf-name   all]</pre> <p><b>Example:</b><br/>Router# show mpls ldp discovery</p>                                                                                                                                 | <p>(Optional) Displays the status of the LDP discovery process.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp discovery</b> command to verify that LDP is operational in the CSC core.</li> </ul>                                                    |
| Step 6  | <pre>show mpls ldp neighbor [[vrf vrf-name] [address   interface] [detail]   all]</pre> <p><b>Example:</b><br/>Router# show mpls ldp neighbor</p>                                                                                                  | <p>(Optional) Displays the status of LDP sessions.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp neighbor</b> command to verify LDP configuration in the CSC core.</li> </ul>                                                                        |
| Step 7  | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef</p>                                                                                                                   | <p>(Optional) Displays entries in the forwarding information base (FIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check the forwarding table (prefixes, next hops, and interfaces).</li> </ul>                                     |
| Step 8  | <pre>show mpls interfaces [[vrf vrf-name] [interface] [detail]   all]</pre> <p><b>Example:</b><br/>Router# show mpls interfaces</p>                                                                                                                | <p>(Optional) Displays information about one or more or all interfaces that are configured for label switching.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls interfaces</b> command to verify that the interfaces are configured to use LDP.</li> </ul> |
| Step 9  | <pre>show ip route</pre> <p><b>Example:</b><br/>Router# show ip route</p>                                                                                                                                                                          | <p>(Optional) Displays IP routing table entries.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, interface, and so forth.</li> </ul>                             |
| Step 10 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                      | <p>(Optional) Returns to privileged EXEC mode.</p>                                                                                                                                                                                                                         |

## Troubleshooting Tips

You can use the **ping** and **trace** commands to verify complete MPLS connectivity in the core. You also get useful troubleshooting information from the additional **show** commands.

## Configuring VRFs for CSC-PE Routers

Perform this task to configure VPN forwarding/routing instances (VRFs) for the backbone carrier edge (CSC-PE) routers.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map** *route-map*
7. **exit**
8. **interface** *type number*
9. **ip vrf forwarding** *vrf-name*
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf vpn1         | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                      |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1 | Creates routing and forwarding tables. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit AS number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul> |

|                | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b>  | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target import 100:1</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| <b>Step 6</b>  | <pre>import map route-map</pre> <p><b>Example:</b><br/>Router(config-vrf)# import map vpn1-route-map</p>                                             | <p>(Optional) Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 7</b>  | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit</p>                                                                                  | <p>(Optional) Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 8</b>  | <pre>interface type number</pre> <p><b>Example:</b><br/>Router(config)# interface Ethernet5/0</p>                                                    | <p>Specifies the interface to configure.</p> <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 9</b>  | <pre>ip vrf forwarding vrf-name</pre> <p><b>Example:</b><br/>Router(config-if)# ip vrf forwarding vpn1</p>                                           | <p>Associates a VRF with the specified interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 10</b> | <pre>end</pre> <p>Router(config-if)# end</p>                                                                                                         | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

### Troubleshooting Tips

Enter a **show ip vrf detail** command and make sure the MPLS VPN is up and associated with the right interfaces.

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier

Perform this task to configure Multiprotocol BGP (MP-BGP) connectivity in the backbone carrier.

### SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default ipv4-unicast**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type*
7. **address-family vpnv4 [unicast]**
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **activate**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                       | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>no bgp default ipv4-unicast</b><br><br><b>Example:</b><br>Router(config-router)# no bgp default ipv4-unicast                                                                   | (Optional) Disables the IPv4 unicast address family on all neighbors. <ul style="list-style-type: none"> <li>Use the <b>no</b> form of the <b>bgp default-unicast</b> command if you are using this neighbor for MPLS routes only.</li> </ul>                                                                                                                                                                                            |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.5.5.5 remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                      |

|         | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>update-source</b> <i>interface-type</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.2.0.0<br>update-source loopback0 | Allows BGP sessions to use a specific operational interface for TCP connections. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument specifies the interface to be used as the source.</li> </ul> |
| Step 7  | <b>address-family</b> <b>vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                                | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                           |
| Step 8  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>send-community</b> <b>extended</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>send-community extended   | Specifies that a communities attribute should be sent to a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP-speaking neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                       |
| Step 9  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.4.0.0<br>activate                                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                          |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                                                         | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                   |

## Troubleshooting Tips

You can enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. If this command is not successful, enter a **debug ip bgp x.x.x.x events** command, where *x.x.x.x* is the IP address of the neighbor.

## Configuring the CSC-PE and CSC-CE Routers

Perform the following tasks to configure and verify links between a CSC-PE router and the carrier CSC-CE router for an MPLS VPN CSC network that uses BGP to distribute routes and MPLS labels.

- [Configuring CSC-PE Routers, page 13](#) (required)
- [Configuring CSC-CE Routers, page 15](#) (required)
- [Verifying Labels in the CSC-PE Routers, page 17](#) (optional)

- [Verifying Labels in the CSC-CE Routers, page 19](#) (optional)

Figure 3 shows the configuration for the peering with directly connected interfaces between CSC-PE and CSC-CE routers. This configuration is used as the example in the tasks that follow.

**Figure 3** Configuration for Peering with Directly Connected Interfaces Between CSC-PE and CSC-CE Routers



## Configuring CSC-PE Routers

Perform this task to configure the CSC-PE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **as-override**
8. **neighbor** *ip-address* **send-label**
9. **exit-address-family**
10. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                              |
|--------|-----------------------------------------------|--------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                        |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                    |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                      |



|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>router</b> <b>bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                         | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                           |
| Step 4 | <b>address-family</b> <b>ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1         | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.2<br>activate                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                 |
| Step 7 | <b>neighbor</b> <i>ip-address</i> <b>as-override</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.2<br>as-override                                                  | Configures a PE router to override the autonomous system number (ASN) of a site with the ASN of a provider. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the router that is to be overridden with the ASN provided.</li> </ul>                                                                                                                                                                                |
| Step 8 | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.2<br>send-label                                                    | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                  | Purpose                                   |
|---------|----------------------------------------------------------------------------------------------------|-------------------------------------------|
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family | Exits address family configuration mode.  |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                    | (Optional) Exits to privileged EXEC mode. |

### Troubleshooting Tips

Enter a **show ip bgp neighbor** command to verify that the neighbors are up and running. Make sure you see the following line in the command output under Neighbor capabilities:

```
IPv4 MPLS Label capability:advertised and received
```

## Configuring CSC-CE Routers

Perform this task to configure the CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **redistribute** *protocol*
6. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** *ip-address* **send-label**
9. **exit-address-family**
10. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                 | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>redistribute protocol</b><br><br><b>Example:</b><br>Router(config-router-af)# redistribute static                                 | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>ospf</b>, <b>mobile</b>, <b>static [ip]</b>, <b>connected</b>, and <b>rip</b>. <ul style="list-style-type: none"> <li>The <b>static [ip]</b> keyword redistributes IP static routes. The optional <b>ip</b> keyword is used when you redistribute static routes into IS-IS.</li> <li>The <b>connected</b> keyword refers to routes which are established automatically when IP is enabled on an interface. For routing protocols such as OSPF and IS-IS, these routes are redistributed as external to the autonomous system.</li> </ul> </li> </ul> |

|         | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.5.0.2<br>remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.3.0.2<br>activate                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 8  | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.2<br>send-label                                                    | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                          |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                         | Exits from the address family configuration mode.                                                                                                                                                                                                                                                                                                                                   |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                            | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                           |

## Verifying Labels in the CSC-PE Routers

Perform this task to verify the labels in the CSC-PE routers.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]
3. **show mpls interfaces** [**all**]
4. **show ip route vrf** *vrf-name* [*prefix*]
5. **show ip bgp vpnv4** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**summary**] [**labels**]
6. **show ip cef** [**vrf** *vrf-name*] [*network* [*mask*]] [**longer-prefixes**] [**detail**]
7. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
8. **traceroute vrf** [*vrf-name*] *ip-address*

## 9. disable

## DETAILED STEPS

|        | Command or Action                                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all summary     | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>show ip bgp vpnv4 all summary</b> command to check that the BGP session is up and running between the CSC-PE routers and the CSC-CE routers. Check the data in the State/PfxRcd column to verify that prefixes are learned during each session.</li> </ul>                                                                                                                                                              |
| Step 3 | <b>show mpls interfaces [all]</b><br><br><b>Example:</b><br>Router# show mpls interfaces all                                                                  | (Optional) Displays information about one or more interfaces that have been configured for label switching. <ul style="list-style-type: none"> <li>Use the <b>show mpls interfaces all</b> command to check that MPLS interfaces are up and running, and that LDP-enabled interfaces show that LDP is up and running. Check that LDP is turned off on the VRF because EBGp distributes the labels.</li> </ul>                                                                                                                             |
| Step 4 | <b>show ip route vrf vrf-name [prefix]</b><br><br><b>Example:</b><br>Router# show ip route vrf vpn1 10.5.5.5                                                  | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use the <b>show ip route vrf</b> command to check that the prefixes for the PE routers are in the routing table of the CSC-PE routers.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p>                                                       |
| Step 5 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [summary] [labels]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 vrf vpn1 labels | (Optional) Displays VPN address information from the BGP table. <ul style="list-style-type: none"> <li>Use the <b>show ip bgp vpnv4 vrf vrf-name labels</b> command to check that the prefixes for the customer carrier MPLS service provider networks are in the BGP table and have the appropriate labels.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p> |

|        | Command or Action                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <pre>show ip cef [vrf vrf-name] [network [mask]] [longer-prefixes] [detail]</pre> <p><b>Example:</b><br/>Router# show ip cef vrf vpn1 10.1.0.0 detail</p>                                                                                                                   | <p>(Optional) Displays entries in the forwarding information base (FIB) or displays a summary of the FIB.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip cef vrf</b> and the <b>show ip cef vrf detail</b> commands to check that the prefixes of the PE routers are in the CEF table.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 7 | <pre>show mpls forwarding-table [vrf vrf-name] [{network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel [tunnel-id]]] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table vrf vpn1 10.1.0.0 detail</p> | <p>(Optional) Displays the contents of the MPLS forwarding information base (LFIB).</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command with the <b>vrf</b> keyword and both the <b>vrf</b> and <b>detail</b> keywords to check that the prefixes for the PE routers in the local customer MPLS VPN service provider are in the LFIB.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p>                                                                                                                                                           |
| Step 8 | <pre>traceroute vrf [vrf-name] ip-address</pre> <p><b>Example:</b><br/>Router# traceroute vrf vpn2 10.2.0.0</p>                                                                                                                                                             | <p>Shows the routes that packets follow traveling through a network to their destination.</p> <ul style="list-style-type: none"> <li>Use the <b>traceroute vrf</b> command to check the data path and transport labels from a PE to a destination CE router.</li> </ul> <p><b>Note</b> This command works with MPLS-aware traceroute only if the backbone routers are configured to propagate and generate IP Time to Live (TTL) information. For more information, see the documentation on the <b>mpls ip propagate-ttl</b> command.</p> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p> |
| Step 9 | <pre>disable</pre> <p><b>Example:</b><br/>Router# disable</p>                                                                                                                                                                                                               | <p>(Optional) Exits to user EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Verifying Labels in the CSC-CE Routers

Perform this task to verify the labels in the CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **show ip bgp summary**
3. **show ip route [address]**

4. **show mpls ldp bindings** [*network* {*mask* | *length*}]
5. **show ip cef** [*network* [*mask*]] [**longer-prefixes**] [**detail**]
6. **show mpls forwarding-table** [**vrf** *vrf-name*] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
7. **show ip bgp labels**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>show ip bgp summary</b><br><br><b>Example:</b><br>Router# show ip bgp summary                                                                                  | (Optional) Displays the status of all BGP connections. <ul style="list-style-type: none"> <li>Use the <b>show ip bgp summary</b> command to check that the BGP session is up and running on the CSC-CE routers.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>show ip route</b> [ <i>address</i> ]<br><br><b>Example:</b><br>Router# show ip route 10.1.0.0                                                                  | (Optional) Displays IP routing table entries. <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to check that the loopback address of the local and remote PE routers are in the routing table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p>                                                                                                          |
| Step 4 | <b>show mpls ldp bindings</b> [ <i>network</i> { <i>mask</i>   <i>length</i> }]<br><br><b>Example:</b><br>Router# show mpls ldp bindings 10.2.0.0 255.255.255.255 | (Optional) Displays the contents of the label information base (LIB). <ul style="list-style-type: none"> <li>Use the <b>show mpls ldp bindings</b> command to check that the prefix of the local PE router is in the MPLS LDP bindings.</li> </ul>                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>show ip cef</b> [ <i>network</i> [ <i>mask</i> ]] [ <b>longer-prefixes</b> ] [ <b>detail</b> ]<br><br><b>Example:</b><br>Router# show ip cef 10.5.0.0 detail   | (Optional) Displays entries in the forwarding information base (FIB) or a summary of the FIB. <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> and the <b>show ip cef detail</b> commands to check that the prefixes of the local and remote PE routers are in the Cisco Express Forwarding table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes and the labels for the same destination learned from the CSC-CE are installed in the corresponding VRF table.</p> |

| Command or Action                                                                                                                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Step 6</b></p> <pre>show mpls forwarding-table [vrf vrf-name] [{network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel {tunnel-id}}] [detail]</pre> <p><b>Example:</b><br/>Router# show mpls forwarding-table 10.2.0.0 detail</p> | <p>(Optional) Displays the contents of the MPLS LFIB.</p> <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> and <b>show mpls forwarding-table detail</b> commands to check that the prefixes of the local and remote PE routers are in the MPLS forwarding table.</li> </ul> <p><b>Note</b> If you have multiple paths configured between CSC-PE and CSC-CE, verify that the multiple routes and labels for the same destination learned from the CSC-CE are installed in the corresponding VRF routing table.</p> |
| <p><b>Step 7</b></p> <pre>show ip bgp labels</pre> <p><b>Example:</b><br/>Router# show ip bgp labels</p>                                                                                                                                                                                | <p>(Optional) Displays information about MPLS labels from the EBGp route table.</p> <ul style="list-style-type: none"> <li>Use the <b>show ip bgp labels</b> command to check that the BGP routing table contains labels for prefixes in the customer carrier MPLS VPN service provider networks.</li> </ul>                                                                                                                                                                                                                                      |

## Configuring the Customer Carrier Network

Perform the following tasks to configure and verify the customer carrier network. This requires setting up connectivity and routing functions for the customer carrier core (P) routers and the customer carrier edge (PE) routers.

- [Verifying IP Connectivity in the Customer Carrier, page 21](#) (optional)
- [Configuring a Customer Carrier Core Router as a Route Reflector, page 22](#) (optional)

## Prerequisites

Before you configure an MPLS VPN CSC network that uses BGP to distribute routes and MPLS labels, you must configure the following on your customer carrier routers:

- An IGP routing protocol—BGP, OSPF, IS-IS, EIGRP, static, and so on. For information, see [Configuring a Basic BGP Network](#), [Configuring OSPF](#), [Configuring a Basic IS-IS Network](#), and [Configuring EIGRP](#).
- MPLS VPN functionality on the PE routers (for hierarchical VPNs only).
- Label Distribution Protocol (LDP) on P and PE routers (for hierarchical VPNs only). For information, see [How to Configure MPLS LDP](#).



### Note

You must configure the items in the preceding list before performing the tasks in this section.

## Verifying IP Connectivity in the Customer Carrier

Perform this task to verify IP connectivity in the customer carrier.



## SUMMARY STEPS

1. **enable**
2. **ping** [*protocol*] {*host-name* | *system-address*}
3. **trace** [*protocol*] [*destination*]
4. **show ip route**
5. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                          |
| Step 2 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system-address</i> }<br><br><b>Example:</b><br>Router# ping ip 10.2.0.0 | Diagnoses basic network connectivity on AppleTalk, CLNS, IP, Novell, Apollo, VINES, DECnet, or XNS networks. <ul style="list-style-type: none"> <li>Use the <b>ping</b> command to verify the connectivity from one customer carrier core router to another.</li> </ul>                                                                                   |
| Step 3 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip 10.1.0.0                     | Discovers the routes that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to verify the path that a packet goes through before reaching the final destination. The <b>trace</b> command can help isolate a trouble spot if two routers cannot communicate.</li> </ul> |
| Step 4 | <b>show ip route</b><br><br><b>Example:</b><br>Router# show ip route                                                            | Displays IP routing table entries. <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> command to display the entire routing table, including host IP address, next hop, interface, and so forth.</li> </ul>                                                                                                                              |
| Step 5 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                        | Returns to user mode.                                                                                                                                                                                                                                                                                                                                     |

## Configuring a Customer Carrier Core Router as a Route Reflector

Perform this task to configure a customer carrier core (P) router as a route reflector of multiprotocol BGP prefixes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*

4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family vpnv4** [**unicast**]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** *ip-address* **route-reflector-client**
8. **exit-address-family**
9. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                             | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and labels the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul> |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.1.1.1<br>remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                        |
| Step 5 | <b>address-family vpnv4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpnv4                                                                    | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The optional <b>unicast</b> keyword specifies VPNv4 unicast address prefixes.</li> </ul>                                                                                                                                                                          |

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.1.1.1<br>activate | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 7 | <b>neighbor</b> <i>ip-address</i> <b>route-reflector-client</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.1.1.1<br>route-reflector-client     | Configures the router as a BGP route reflector and configures the specified neighbor as its client. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the BGP neighbor being identified as a client.</li> </ul>                    |
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                  | Exits address family configuration mode.                                                                                                                                                                                                                                           |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                     | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                          |

## Troubleshooting Tips

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. For neighbors to exchange other address prefix types, such as multicast and VPNv4, you must also activate neighbors using the **neighbor activate** command in address family configuration mode, as shown.

Route reflectors and clients (neighbors or internal BGP peer groups) that are defined in router configuration mode using the **neighbor route-reflector-client** command reflect unicast address prefixes to and from those clients by default. To cause them to reflect prefixes for other address families, such as multicast, define the reflectors and clients in address family configuration mode, using the **neighbor route-reflector-client** command, as shown.

## Configuring the Customer Site for Hierarchical VPNs



### Note

This section applies only to customer carrier networks that use BGP to distribute routes and MPLS labels.

Perform the following tasks to configure and verify the customer site for hierarchical VPNs:

- [Defining VPNs on PE Routers for Hierarchical VPNs, page 25](#) (required)
- [Configuring BGP Routing Sessions on the PE Routers for Hierarchical VPNs, page 26](#) (required)
- [Verifying Labels in Each PE Router for Hierarchical VPNs, page 28](#) (optional)
- [Configuring CE Routers for Hierarchical VPNs, page 29](#) (required)
- [Verifying IP Connectivity in the Customer Site, page 31](#) (optional)

**Note**

This section applies to hierarchical VPNs only.

## Defining VPNs on PE Routers for Hierarchical VPNs

Perform this task to define VPNs on PE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **import map** *route-map*
7. **ip vrf forwarding** *vrf-name*
8. **exit**

### DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                |
|--------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                      |
| Step 3 | <b>ip vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# ip vrf vpn2         | Creates a VRF routing table and a Cisco Express Forwarding table and enters VRF configuration mode.<br><ul style="list-style-type: none"> <li>• The <i>vrf-name</i> argument is a name you assign to a VRF.</li> </ul> |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# rd 200:1 | Creates routing and forwarding tables for a VRF.<br><ul style="list-style-type: none"> <li>• The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.</li> </ul>    |

|        | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>route-target {import   export   both} route-target-ext-community</pre> <p><b>Example:</b><br/>Router(config-vrf)# route-target export 200:1</p> | <p>Creates a route-target extended community for a VRF.</p> <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul> |
| Step 6 | <pre>import map route-map</pre> <p><b>Example:</b><br/>Router(config-vrf)# import map map23</p>                                                      | <p>Configures an import route map for a VRF.</p> <ul style="list-style-type: none"> <li>The <i>route-map</i> argument specifies the route map to be used as an import route map for the VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 7 | <pre>ip vrf forwarding vrf-name</pre> <p><b>Example:</b><br/>Router(config-vrf)# ip vrf forwarding vpn2</p>                                          | <p>Associates a VPN VRF instance with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8 | <pre>exit</pre> <p><b>Example:</b><br/>Router(config-vrf)# exit</p>                                                                                  | <p>Exits to global configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Configuring BGP Routing Sessions on the PE Routers for Hierarchical VPNs

Perform this task to configure BGP routing sessions on the PE routers for PE-to-CE router communication.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **neighbor** {*ip address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                           | Configures the router to run a BGP process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                 |
| Step 4 | <b>address-family ipv4 [<i>multicast</i>   <i>unicast</i>   <i>vrf vrf-name</i>]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 multicast                   | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf <i>vrf-name</i></b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>}</b><br><b>remote-as <i>as-number</i></b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.5.5.5 remote-as 300 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                |

|        | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.1.0.0<br>activate | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                  | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                      |

## Verifying Labels in Each PE Router for Hierarchical VPNs

Perform this task to verify labels in each PE router for hierarchical VPNs.

### SUMMARY STEPS

1. **enable**
2. **show ip route vrf vrf-name** [*prefix*]
3. **show mpls forwarding-table** [*vrf vrf-name*] [*prefix*] [*detail*]
4. **show ip cef** [*network* [*mask* [*longer-prefix*]]] [*detail*]
5. **show ip cef vrf vrf-name** [*ip-prefix*]
6. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                       |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                              |
| Step 2 | <b>show ip route vrf vrf-name</b> [ <i>prefix</i> ]<br><br><b>Example:</b><br>Router# show ip route vrf vpn2 10.5.5.5                                                        | (Optional) Displays the IP routing table associated with a VRF. <ul style="list-style-type: none"> <li>Use the <b>show ip route vrf</b> command to check that the loopback addresses of the local and remote CE routers are in the routing table of the PE routers.</li> </ul>                |
| Step 3 | <b>show mpls forwarding-table</b> [ <i>vrf vrf-name</i> ] [ <i>prefix</i> ] [ <i>detail</i> ]<br><br><b>Example:</b><br>Router# show mpls forwarding-table vrf vpn2 10.1.0.0 | (Optional) Displays the contents of the LFIB. <ul style="list-style-type: none"> <li>Use the <b>show mpls forwarding-table</b> command to check that the prefixes for the local and remote CE routers are in the MPLS forwarding table, and that the specified prefix is untagged.</li> </ul> |

|        | Command or Action                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                        |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>show ip cef</b> [ <i>network</i> [ <i>mask</i> [ <i>longer-prefix</i> ]]] [ <i>detail</i> ]<br><br><b>Example:</b><br>Router# show ip cef 10.2.0.0 | (Optional) Displays specific entries in the FIB based on IP address information. <ul style="list-style-type: none"> <li>Use the <b>show ip cef</b> command to check that the prefixes of the local and remote PE routers are in the Cisco Express Forwarding table.</li> </ul> |
| Step 5 | <b>show ip cef vrf</b> <i>vrf-name</i> [ <i>ip-prefix</i> ]<br><br><b>Example:</b><br>Router# show ip cef vrf vpn2 10.3.0.0                           | (Optional) Displays the Cisco Express Forwarding table associated with a VRF. <ul style="list-style-type: none"> <li>Use the <b>show ip cef vrf</b> command to check that the prefix of the remote CE router is in the Cisco Express Forwarding table.</li> </ul>              |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                    | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                            |

## Configuring CE Routers for Hierarchical VPNs

Perform this task to configure CE routers for hierarchical VPNs. This configuration is the same as that for an MPLS VPN that is not in a hierarchical topology.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef** [*distributed*]
4. **interface** *type number*
5. **ip address** *ip-address mask* [*secondary*]
6. **exit**
7. **router bgp** *as-number*
8. **redistribute** *protocol*
9. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
10. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>ip cef [distributed]</b><br><br><b>Example:</b><br>Router(config)# ip cef distributed                                       | Enables Cisco Express Forwarding on the route processor card. <ul style="list-style-type: none"> <li>The <b>distributed</b> keyword enables distributed Cisco Express Forwarding operation. Cisco Express Forwarding information is distributed to the line cards. Line cards perform express forwarding.</li> </ul> <b>Note</b> For the Cisco ASR 1000 Series Aggregation Services Router, the <b>distributed</b> keyword is required.                                                                                                                                                                     |
| Step 4 | <b>interface type number</b><br><br><b>Example:</b><br>Router(config)# interface loopback 0                                    | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured. <ul style="list-style-type: none"> <li>A loopback interface indicates a software-only interface that emulates an interface that is always up. It is a virtual interface supported on all platforms.</li> </ul> </li> <li>The <i>number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.</li> </ul> |
| Step 5 | <b>ip address ip-address mask [secondary]</b><br><br><b>Example:</b><br>Router(config-if)# ip address 10.8.0.0 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul>                                                                                                                                                                               |
| Step 6 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                  | Exits interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <code>router bgp as-number</code><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                   | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                                                                                                                                                                                                                |
| Step 8  | <code>redistribute protocol</code><br><br><b>Example:</b><br>Router(config-router)# redistribute connected                                                                   | Redistributes routes from one routing domain into another routing domain. <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>connected</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>mobile</b>, <b>ospf</b>, <b>static</b> [ip], or <b>rip</b>.</li> </ul> <p>The <b>connected</b> keyword refers to routes that are established automatically when IP is enabled on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes are redistributed as external to the autonomous system.</p> |
| Step 9  | <code>neighbor {ip-address   peer-group-name}</code><br><code>remote-as as-number</code><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.8.0.0<br>remote-as 100 | Adds the IP address of the neighbor in the remote autonomous system to the multiprotocol BGP neighbor table of the local router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                  |
| Step 10 | <code>end</code><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                        | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Verifying IP Connectivity in the Customer Site

Perform this task to verify IP connectivity in the customer site.

### SUMMARY STEPS

- enable**
- show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]
- ping** [*protocol*] {*host-name* | *system-address*}
- trace** [*protocol*] [*destination*]
- disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>show ip route</b> [ <i>ip-address</i> [ <i>mask</i> ]<br>[ <b>longer-prefixes</b> ]   <i>protocol</i> [ <i>process-id</i> ]  <br><b>list</b> [ <i>access-list-number</i>   <i>access-list-name</i> ]  <br><b>static download</b> ]<br><br><b>Example:</b><br>Router# show ip route 10.5.5.5 | (Optional) Displays the current state of the routing table. <ul style="list-style-type: none"> <li>Use the <b>show ip route</b> <i>ip-address</i> command to check that the loopback addresses of the remote CE routers learned through the PE router are in the routing table of the local CE routers.</li> </ul>                                                                                                                                     |
| Step 3 | <b>ping</b> [ <i>protocol</i> ] { <i>host-name</i>   <i>system-address</i> }<br><br><b>Example:</b><br>Router# ping 10.5.5.5                                                                                                                                                                   | Diagnoses basic network connectivity on Apollo, AppleTalk, Connectionless Network Service (CLNS), DECnet, IP, Novell IPX, VINES, or XNS networks. <ul style="list-style-type: none"> <li>Use the <b>ping</b> command to check connectivity between customer site routers.</li> </ul>                                                                                                                                                                   |
| Step 4 | <b>trace</b> [ <i>protocol</i> ] [ <i>destination</i> ]<br><br><b>Example:</b><br>Router# trace ip 10.5.5.5                                                                                                                                                                                    | Discovers the routes that packets will actually take when traveling to their destination. <ul style="list-style-type: none"> <li>Use the <b>trace</b> command to follow the path of the packets in the customer site.</li> <li>To use nondefault parameters and invoke an extended <b>trace</b> test, enter the <b>trace</b> command without a destination argument. You will be stepped through a dialog to select the desired parameters.</li> </ul> |
| Step 5 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                                       | (Optional) Exits to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuration Examples for MPLS VPN CSC with BGP

Configuration examples for the MPLS VPN CSC with BGP include the following:

- [Configuring the Backbone Carrier Core: Examples, page 33](#)
- [Configuring the Links Between CSC-PE and CSC-CE Routers: Examples, page 36](#)
- [Configuring the Customer Carrier Network: Examples, page 43](#)
- [Configuring the Customer Site for Hierarchical VPNs: Examples, page 44](#)

Figure 4 shows a sample CSC topology for exchanging IPv4 routes and MPLS labels. Use this figure as a reference for configuring and verifying carrier supporting carrier routers to exchange IPv4 routes and MPLS labels.

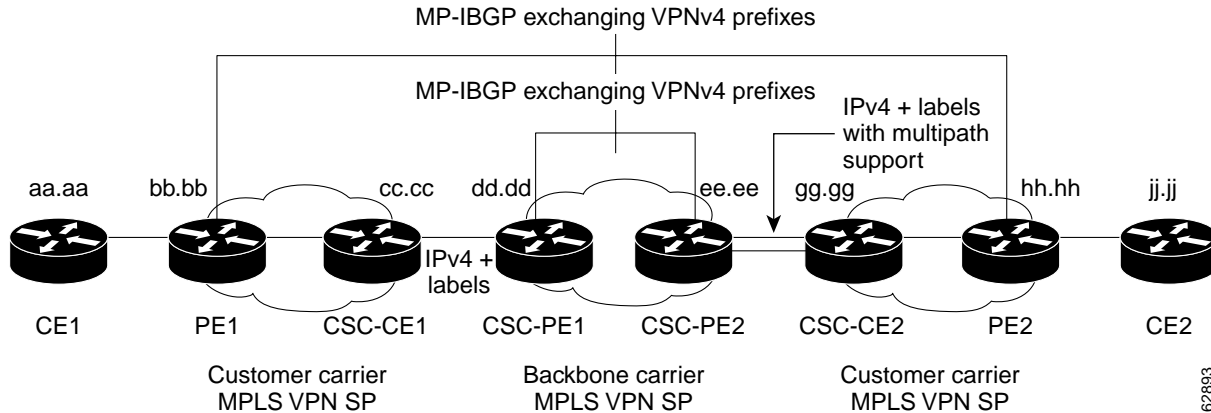
**Figure 4**      **Sample CSC Topology for Exchanging IPv4 Routes and MPLS Labels**

Table 1 describes the sample configuration shown in Figure 4.

**Table 1**      **Description of Sample Configuration Shown in Figure 4**

| Routers             | Description                                                                                                                                                                                                                                                                                                                                                           |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CE1 and CE2         | <p>Belong to an end customer. CE1 and CE2 routers exchange routes learned from PE routers.</p> <p>The end customer is purchasing VPN services from a customer carrier.</p>                                                                                                                                                                                            |
| PE1 and PE2         | <p>Part of a customer carrier network that is configured to provide MPLS VPN services. PE1 and PE2 are peering with a VPNv4 IBGP session to form an MPLS VPN network.</p>                                                                                                                                                                                             |
| CSC-CE1 and CSC-CE2 | <p>Part of a customer carrier network. CSC-CE1 and CSC-CE2 routers exchange IPv4 BGP updates with MPLS labels and redistribute PE loopback addressees to and from the IGP (OSPF in this example).</p> <p>The customer carrier is purchasing carrier supporting carrier VPN services from a backbone carrier.</p>                                                      |
| CSC-PE1 and CSC-PE2 | <p>Part of the backbone carrier's network configured to provide carrier supporting carrier VPN services. CSC-PE1 and CSC-PE2 are peering with a VPNv4 IP BGP session to form the MPLS VPN network. In the VRF, CSC-PE1 and CSC-PE2 are peering with the CSC-CE routers, which are configured for carrying MPLS labels with the routes, with an IPv4 EBGP session.</p> |

## Configuring the Backbone Carrier Core: Examples

Configuration and verification examples for the backbone carrier core included in this section are as follows:

- [Verifying IP Connectivity and LDP Configuration in the CSC Core: Example, page 34](#)
- [Configuring VRFs for CSC-PE Routers: Example, page 35](#)
- [Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier: Example, page 35](#)

## Verifying IP Connectivity and LDP Configuration in the CSC Core: Example

Check that CSC-PE2 is reachable from CSC-PE1 by entering the following command on CSC-CE1:

```
Router# ping 10.5.5.5
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.5.5.5, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

Verify the path from CSC-PE1 to CSC-PE2 by entering the following command on CSC-CE1:

```
Router# trace 10.5.5.5
```

Type escape sequence to abort.

Tracing the route to 10.5.5.5

```
  1 10.5.5.5 0 msec 0 msec *
```

Check that CSC-PE router prefixes are in the MPLS forwarding table:

```
Router# show mpls forwarding-table
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop    |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 16        | 2/nn               | dd.dd.dd.dd/32      | 0                  | AT2/1/0.1          | point2point |
| 17        | 16                 | bb.bb.bb.bb/32[V]   | 30204              | Et1/0              | pp.0.0.1    |
| 21        | Pop tag            | cc.cc.cc.cc/32[V]   | 0                  | Et1/0              | pp.0.0.1    |
| 22        | Pop tag            | nn.0.0.0/8[V]       | 570                | Et1/0              | pp.0.0.1    |
| 23        | Aggregate          | pp.0.0.0/8[V]       | 0                  |                    |             |
| 2         | 2/nn               | gg.gg.gg.gg/32[V]   | 0                  | AT3/0.1            | point2point |
| 8         | 2/nn               | hh.hh.hh.hh/32[V]   | 15452              | AT3/0.1            | point2point |
| 29        | 2/nn               | qq.0.0.0/8[V]       | 0                  | AT3/0.1            | point2point |
| 30        | 2/nn               | ss.0.0.0/8[V]       | 0                  | AT3/0.1            | point2point |

Check the status of LDP discovery processes in the core:

```
Router# show mpls ldp discovery
```

Local LDP Identifier:

ee.00.00.00:0

Discovery Sources:

Interfaces:

ATM2/1/0.1 (ldp): xmit/rcv

TDP Id: dd.dd.dd.dd:1

Check the status of LDP sessions in the core:

```
Router# show mpls ldp neighbor
```

Peer LDP Ident: dd.dd.dd.dd:1; Local LDP Ident ee.00.00.00:1

TCP connection: dd.dd.dd.dd.646 - ee.00.00.00.11007

State: Oper; Msgs sent/rcvd: 20/21; Downstream on demand

Up time: 00:14:56

LDP discovery sources:

ATM2/1/0.1, Src IP addr: dd.dd.dd.dd

Check the forwarding table (prefixes, next-hops, and interfaces):

```
Router# show ip cef
```

| Prefix    | Next Hop | Interface                           |
|-----------|----------|-------------------------------------|
| 0.0.0.0/0 | drop     | Null0 (default route handler entry) |

```

0.0.0.0/32          receive
dd.dd.dd.dd/32      dd.dd.dd.dd      ATM2/1/0.1
ee.aa.aa.aa/32      receive
224.0.0.0/4         drop
224.0.0.0/24        receive
255.255.255.255/32 receive

```

**Note**

Also see the [“Verifying Labels in the CSC-CE Routers: Examples”](#) section on page 41.

Verify that interfaces are configured to use LDP:

```
Router# show mpls interfaces
```

| Interface   | IP        | Tunnel | Operational |
|-------------|-----------|--------|-------------|
| Ethernet0/1 | Yes (ldp) | No     | Yes         |

Display the entire routing table, including host IP address, next hop, interface, and so forth:

```
Router# show ip route
```

```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR

```

Gateway of last resort is not set

```

          dd.0.0.0/32 is subnetted, 1 subnets
O          dd.dd.dd.dd [110/7] via dd.dd.dd.dd, 00:16:42, ATM2/1/0.1
          ee.0.0.0/32 is subnetted, 1 subnets
C          ee.aa.aa.aa is directly connected, Loopback0

```

## Configuring VRFs for CSC-PE Routers: Example

The following example shows how to configure a VPN routing and forwarding (VRF) instance for a CSC-PE router:

```

ip cef distributed

ip vrf vpn1
rd 100:1
route target both 100:1
!

```

## Configuring Multiprotocol BGP for VPN Connectivity in the Backbone Carrier: Example

The following example shows how to configure Multiprotocol BGP (MP-BGP) for VPN connectivity in the backbone carrier:

```

ip cef distributed

ip vrf vpn1
rd 100:1
route target both 100:1

hostname csc-pe1

```

```

!
router bgp 100
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor ee.aa.aa.aa remote-as 100
  neighbor ee.aa.aa.aa update-source Loopback0
  no auto-summary
!
address-family vpnv4
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa send-community extended
  bgp dampening 30
  exit-address-family
!
router bgp 100
. . .
! (BGP IPv4 to CSC-CE router from CSC-PE router)
!
address-family ipv4 vrf vpn1
  neighbor ss.0.0.2 remote-as 200
  neighbor ss.0.0.2 activate
  neighbor ss.0.0.2 as-override
  neighbor ss.0.0.2 advertisement-interval 5
  neighbor ss.0.0.2 send-label
  no auto-summary
  no synchronization
  bgp dampening 30
  exit-address-family
!

```

## Configuring the Links Between CSC-PE and CSC-CE Routers: Examples

This section contains the following examples:

- [Configuring the CSC-PE Routers: Examples, page 36](#)
- [Configuring the CSC-CE Routers: Examples, page 37](#)
- [Verifying Labels in the CSC-PE Routers: Examples, page 38](#)
- [Verifying Labels in the CSC-CE Routers: Examples, page 41](#)

## Configuring the CSC-PE Routers: Examples

The following example shows how to configure a CSC-PE router:

```

ip cef
!
ip vrf vpn1
  rd 100:1
  route-target export 100:1
  route-target import 100:1
mpls label protocol ldp
!
interface Loopback0
  ip address dd.dd.dd.dd 255.255.255.255
!
interface Ethernet3/1
  ip vrf forwarding vpn1
  ip address pp.0.0.2 255.0.0.0
!

```

```

interface ATM0/1/0
  no ip address
  no ip directed-broadcast
  no ip route-cache distributed
  atm clock INTERNAL
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM0/1/0.1 mpls
  ip unnumbered Loopback0
  no ip directed-broadcast
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls atm vpi 2-5
  mpls ip
!
router ospf 100
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  redistribute connected subnets
  passive-interface Ethernet3/1
  network dd.dd.dd.dd 0.0.0.0 area 100
!
router bgp 100
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  timers bgp 10 30
  neighbor ee.aa.aa.aa remote-as 100
  neighbor ee.aa.aa.aa update-source Loopback0
!
address-family vpnv4                                     !VPNv4 session with CSC-PE2
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa send-community extended
  bgp dampening 30
  exit-address-family
!
address-family ipv4 vrf vpn1
  neighbor pp.0.0.1 remote-as 200
  neighbor pp.0.0.1 activate
  neighbor pp.0.0.1 as-override
  neighbor pp.0.0.1 advertisement-interval 5
  neighbor pp.0.0.1 send-label
  no auto-summary
  no synchronization
  bgp dampening 30
  exit-address-family

```

## Configuring the CSC-CE Routers: Examples

The following example shows how to configure a CSC-CE router:

```

ip cef
!
mpls label protocol ldp
!
interface Loopback0
  ip address cc.cc.cc.cc 255.255.255.255
!
interface Ethernet3/0
  ip address pp.0.0.1 255.0.0.0
!
interface Ethernet4/0
  ip address nn.0.0.2 255.0.0.0

```



```

no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
redistribute connected subnets           !Exchange routes
redistribute bgp 200 metric 3 subnets     !learned from PE1
passive-interface ATM1/0
passive-interface Ethernet3/0
network cc.cc.cc.cc 0.0.0.0 area 200
network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
timers bgp 10 30
neighbor pp.0.0.2 remote-as 100
neighbor pp.0.0.2 update-source Ethernet3/0
no auto-summary
!
address-family ipv4
redistribute connected
redistribute ospf 200 metric 4 match internal
neighbor pp.0.0.2 activate
neighbor pp.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## Verifying Labels in the CSC-PE Routers: Examples

The following examples show how to verify the configurations of the CSC-PE routers.

Verify that the BGP session is up and running between the CSC-PE router and the CSC-CE router. Check the data in the State/PfxRcd column to verify that prefixes are learned during each session.

Router# **show ip bgp vpnv4 all summary**

```

BBGP router identifier 10.5.5.5, local AS number 100
BGP table version is 52, main routing table version 52
12 network entries and 13 paths using 2232 bytes of memory
6 BGP path attribute entries using 336 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 16/4 prefixes, 27/14 paths, scan interval 5 secs

```

| Neighbor | V | AS  | MsgRcvd | MsgSent | TblVer | InQ | OutQ | Up/Down  | State/PfxRcd |
|----------|---|-----|---------|---------|--------|-----|------|----------|--------------|
| 10.5.5.5 | 4 | 100 | 7685    | 7686    | 52     | 0   | 0    | 21:17:04 | 6            |
| 10.0.0.2 | 4 | 200 | 7676    | 7678    | 52     | 0   | 0    | 21:16:43 | 7            |

Verify that the MPLS interfaces are up and running, and that LDP-enabled interfaces show that LDP is up and running. LDP is turned off on the VRF because EBGp distributes the labels.

Router# **show mpls interfaces all**

| Interface          | IP        | Tunnel | Operational |
|--------------------|-----------|--------|-------------|
| GigabitEthernet6/0 | Yes (ldp) | No     | Yes         |

| VRF         | Operational |
|-------------|-------------|
| vpn1:       |             |
| Ethernet3/1 | Yes         |

Verify that the prefix for the local PE router is in the routing table of the CSC-PE router:

```
Router# show ip route vrf vpn2 10.5.5.5
```

```
Routing entry for 10.5.5.5/32
  Known via "bgp 100", distance 20, metric 4
  Tag 200, type external
  Last update from pp.0.0.2 21:28:39 ago
  Routing Descriptor Blocks:
    * pp.0.0.2, from pp.0.0.2, 21:28:39 ago
      Route metric is 4, traffic share count is 1
      AS Hops 1, BGP network version 0
```

Verify that the prefix for the remote PE router is in the routing table of the CSC-PE router:

```
Router# show ip route vrf vpn2 10.5.5.5
```

```
Routing entry for 10.5.5.5/32
  Known via "bgp 100", distance 200, metric 4
  Tag 200, type internal
  Last update from 10.1.0.0 21:27:39 ago
  Routing Descriptor Blocks:
    * 10.1.0.0 (Default-IP-Routing-Table), from 10.1.0.0, 21:27:39 ago
      Route metric is 4, traffic share count is 1
      AS Hops 1, BGP network version 0
```

Verify that the prefixes for the customer carrier MPLS VPN service provider networks are in the BGP table, and have appropriate labels:

```
Router# show ip bgp vpnv4 vrf vpn2 labels
```

| Network                           | Next Hop | In label/Out label |
|-----------------------------------|----------|--------------------|
| Route Distinguisher: 100:1 (vpn1) |          |                    |
| cc.cc.cc.cc/32                    | pp.0.0.2 | 22/imp-null        |
| bb.bb.bb.bb/32                    | pp.0.0.2 | 27/20              |
| hh.hh.hh.hh/32                    | ee.0.0.0 | 34/35              |
| gg.gg.gg.gg/32                    | ee.0.0.0 | 30/30              |
| nn.0.0.0                          | pp.0.0.2 | 23/imp-null        |
| ss.0.0.0                          | ee.0.0.0 | 33/34              |
| pp.0.0.0                          | pp.0.0.2 | 25/aggregate(vpn1) |

Verify that the prefix of the PE router in the local customer carrier MPLS VPN service provider is in the Cisco Express Forwarding table:

```
Router# show ip cef vrf vpn2 10.1.0.0
```

```
10.1.0.0/32, version 19, cached adjacency pp.0.0.2
0 packets, 0 bytes
  tag information set
    local tag: 27
    fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
  via pp.0.0.2, 0 dependencies, recursive
  next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
  valid cached adjacency
  tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
```

```
Router# show ip cef vrf vpn2 10.1.0.0 detail
```

```

10.1.0.0/32, version 19, cached adjacency pp.0.0.2
0 packets, 0 bytes
tag information set
  local tag: 27
  fast tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}
via pp.0.0.2, 0 dependencies, recursive
next hop pp.0.0.2, Ethernet3/1 via pp.0.0.2/32
valid cached adjacency
tag rewrite with Et3/1, pp.0.0.2, tags imposed {20}

```

Verify that the prefix of the PE router in the local customer carrier MPLS VPN service provider is in the MPLS forwarding table:

```
Router# show mpls forwarding-table vrf vpn2 10.1.0.0
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 27        | 20                 | 10.1.0.0/32[V]      | 958048             | Et3/1              | pp.0.0.2 |

```
Router# show mpls forwarding-table vrf vpn2 10.1.0.0 detail
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 27        | 20                 | 10.1.0.0/32[V]      | 958125             | Et3/1              | pp.0.0.2 |

MAC/Encaps=14/18, MTU=1500, Tag Stack{20}  
00B04A74A05400B0C26E10558847 00014000  
VPN route: vpn1  
No output feature configured  
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Verify that the prefix of the PE router in the remote customer carrier MPLS VPN service provider is in the Cisco Express Forwarding table:

```
Router# show ip cef vrf vpn2 10.3.0.0
```

```

10.3.0.0/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
tag information set
  local tag: 34
  fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
via ee.0.0.0, 0 dependencies, recursive
next hop rr.0.0.2, GigabitEthernet6/0 via ee.0.0.0/32
valid cached adjacency
tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}

```

```
Router# show ip cef vrf vpn2 10.3.0.0 detail
```

```

hh.hh.hh.hh/32, version 25, cached adjacency rr.0.0.2
0 packets, 0 bytes
tag information set
  local tag: 34
  fast tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}
via ee.0.0.0, 0 dependencies, recursive
next hop rr.0.0.2, GigabitEthernet6/0 via ee.0.0.0/32
valid cached adjacency
tag rewrite with Gi6/0, rr.0.0.2, tags imposed {35}

```

Verify that the prefix of the PE router in the remote customer carrier MPLS VPN service provider is in the MPLS forwarding table:

```
Router# show mpls forwarding-table vrf vpn2 10.3.0.0
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
|-----------|--------------------|---------------------|--------------------|--------------------|----------|

```

tag      tag or VC      or Tunnel Id      switched      interface
34       35             hh.hh.hh.hh/32[V] 139034        Gi6/0         rr.0.0.2

```

```
Router# show mpls forwarding-table vrf vpn2 10.3.0.0 detail
```

```

Local   Outgoing   Prefix               Bytes tag   Outgoing   Next Hop
tag     tag or VC     or Tunnel Id         switched   interface
34      35           hh.hh.hh.hh/32[V] 139034      Gi6/0      rr.0.0.2
        MAC/Encaps=14/18, MTU=1500, Tag Stack{35}
        00B0C26E447000B0C26E10A88847 00023000
        VPN route: vpn1
        No output feature configured
        Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

```

## Verifying Labels in the CSC-CE Routers: Examples

The following examples show how to verify the configurations of the CSC-CE routers.

Verify that the BGP session is up and running:

```
Router# show ip bgp summary
```

```

BGP router identifier cc.cc.cc.cc, local AS number 200
BGP table version is 35, main routing table version 35
14 network entries and 14 paths using 2030 bytes of memory
3 BGP path attribute entries using 168 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 1 history paths, 0 dampened paths
BGP activity 17/67 prefixes, 29/15 paths, scan interval 60 secs

```

```

Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
pp.0.0.1      4      100    7615    7613     35    0    0 21:06:19      5

```

Verify that the loopback address of the local PE router is in the routing table:

```
Router# show ip route 10.1.0.0
```

```

Routing entry for 10.1.0.0/32
  Known via "ospf 200", distance 110, metric 101, type intra area
  Redistributing via bgp 200
  Advertised by bgp 200 metric 4 match internal
  Last update from nn.0.0.1 on Ethernet4/0, 00:34:08 ago
  Routing Descriptor Blocks:
    * nn.0.0.1, from bb.bb.bb.bb, 00:34:08 ago, via Ethernet4/0
      Route metric is 101, traffic share count is 1

```

Verify that the loopback address of the remote PE router is in the routing table:

```
Router# show ip route 10.5.5.5
```

```

Routing entry for 10.5.5.5/32
  Known via "bgp 200", distance 20, metric 0
  Tag 100, type external
  Redistributing via ospf 200
  Advertised by ospf 200 metric 3 subnets
  Last update from pp.0.0.1 00:45:16 ago
  Routing Descriptor Blocks:
    * pp.0.0.1, from pp.0.0.1, 00:45:16 ago
      Route metric is 0, traffic share count is 1
      AS Hops 2, BGP network version 0

```

Verify that the prefix of the local PE router is in the MPLS LDP bindings:

```
Router# show mpls ldp bindings 10.1.0.0 255.255.255.255
```

```
tib entry: 10.1.0.0/32, rev 20
  local binding: tag: 20
  remote binding: tsr: 10.1.0.0:0, tag: imp-null
```

Verify that the prefix of the local PE router is in the Cisco Express Forwarding table:

```
Router# show ip cef 10.1.0.0
```

```
10.1.0.0/32, version 46, cached adjacency nn.0.0.1
0 packets, 0 bytes
  tag information set
    local tag: 20
  via nn.0.0.1, Ethernet4/0, 0 dependencies
    next hop nn.0.0.1, Ethernet4/0
    unresolved
    valid cached adjacency
    tag rewrite with Et4/0, nn.0.0.1, tags imposed {}
```

Verify that the prefix of the local PE router is in the MPLS forwarding table:

```
Router# show mpls forwarding-table 10.1.0.0
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 20        | Pop tag            | bb.bb.bb.bb/32      | 893397             | Et4/0              | nn.0.0.1 |

```
Router# show mpls forwarding-table 10.1.0.0 detail
```

| Local tag                                                             | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------------------------------------------------------------------|--------------------|---------------------|--------------------|--------------------|----------|
| 20                                                                    | Pop tag            | bb.bb.bb.bb/32      | 893524             | Et4/0              | nn.0.0.1 |
| MAC/Encaps=14/14, MTU=1504, Tag Stack{}                               |                    |                     |                    |                    |          |
| 00074F83685400B04A74A0708847                                          |                    |                     |                    |                    |          |
| No output feature configured                                          |                    |                     |                    |                    |          |
| Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 |                    |                     |                    |                    |          |

Verify that the BGP routing table contains labels for prefixes in the customer carrier MPLS VPN service provider networks:

```
Router# show ip bgp labels
```

| Network        | Next Hop | In Label/Out Label |
|----------------|----------|--------------------|
| cc.cc.cc.cc/32 | 0.0.0.0  | imp-null/exp-null  |
| bb.bb.bb.bb/32 | nn.0.0.1 | 20/exp-null        |
| hh.hh.hh.hh/32 | pp.0.0.1 | 26/34              |
| gg.gg.gg.gg/32 | pp.0.0.1 | 23/30              |
| nn.0.0.0       | 0.0.0.0  | imp-null/exp-null  |
| ss.0.0.0       | pp.0.0.1 | 25/33              |
| pp.0.0.0       | 0.0.0.0  | imp-null/exp-null  |
| pp.0.0.1/32    | 0.0.0.0  | 16/exp-null        |

Verify that the prefix of the remote PE router is in the Cisco Express Forwarding table:

```
Router# show ip cef 10.5.5.5
```

```
10.5.5.5/32, version 54, cached adjacency pp.0.0.1
0 packets, 0 bytes
  tag information set
    local tag: 26
    fast tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}
  via pp.0.0.1, 0 dependencies, recursive
```

```

next hop pp.0.0.1, Ethernet3/0 via pp.0.0.1/32
valid cached adjacency
tag rewrite with Et3/0, pp.0.0.1, tags imposed {34}

```

Verify that the prefix of the remote PE router is in the MPLS forwarding table:

```
Router# show mpls forwarding-table 10.5.5.5
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 26        | 34                 | hh.hh.hh.hh/32      | 81786              | Et3/0              | pp.0.0.1 |

```
Router# show mpls forwarding-table 10.5.5.5 detail
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 26        | 34                 | hh.hh.hh.hh/32      | 81863              | Et3/0              | pp.0.0.1 |

MAC/Encaps=14/18, MTU=1500, Tag Stack{34}  
00B0C26E105500B04A74A0548847 00022000  
No output feature configured  
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

## Configuring the Customer Carrier Network: Examples

Customer carrier configuration and verification examples in this section include:

- [Verifying IP Connectivity in the Customer Carrier: Example, page 43](#)
- [Configuring a Customer Carrier Core Router as a Route Reflector: Example, page 44](#)

### Verifying IP Connectivity in the Customer Carrier: Example

Verify the connectivity from one customer carrier core router to another (from CE1 to CE2) by entering the following command:

```
Router# ping 10.2.0.0
```

```

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.2.0.0, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/9/12 ms

```

Verify the path that a packet goes through on its way to its final destination from CE1 to CE2:

```
Router# trace 10.2.0.0
```

```

Type escape sequence to abort.
Tracing the route to 10.2.0.0

 0 10.0.0.2 0 msec 0 msec 4 msec
 1 10.0.0.2 [MPLS: Labels 20/21 Exp 0] 8 msec 8 msec 12 msec
 2 10.0.0.2 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 12 msec
 3 10.0.0.1 [MPLS: Labels 17/21 Exp 0] 8 msec 8 msec 12 msec
 4 10.0.0.2 [MPLS: Labels 16/21 Exp 0] 8 msec 8 msec 12 msec
 5 10.0.0.1 [AS 200] [MPLS: Label 21 Exp 0] 8 msec 8 msec 8 msec
 6 10.0.0.2 [AS 200] 8 msec 4 msec *

```

Verify the path that a packet goes through on its way to its final destination from CE2 to CE1:

```
Router# trace 10.1.0.0
```

Type escape sequence to abort.  
Tracing the route to 10.1.0.0

```

 1 tt.0.0.1 0 msec 0 msec 0 msec
 2 qq.0.0.2 [MPLS: Labels 18/21 Exp 0] 8 msec 12 msec 12 msec
 3 ss.0.0.1 [MPLS: Labels 28/21 Exp 0] 8 msec 8 msec 8 msec
 4 pp.0.0.2 [MPLS: Labels 17/21 Exp 0] 12 msec 8 msec 8 msec
 5 pp.0.0.1 [MPLS: Labels 16/21 Exp 0] 12 msec 12 msec 8 msec
 6 mm.0.0.2 [AS 200] [MPLS: Label 21 Exp 0] 12 msec 8 msec 12 msec
 7 mm.0.0.1 [AS 200] 4 msec 4 msec *
```

## Configuring a Customer Carrier Core Router as a Route Reflector: Example

The following example shows how to use an address family to configure internal BGP peer 10.1.1.1 as a route-reflector client for both unicast and multicast prefixes:

```

router bgp 200
 address-family vpnv4
  neighbor 10.1.1.1 activate
  neighbor 10.1.1.1 route-reflector-client

router bgp 100
 address-family vpnv4
  neighbor xx.xx.xx.xx activate
  neighbor xx.xx.xx.xx route-reflector-client
  ! xx.xx.xx.xx is a PE router
  neighbor xx.xx.xx.xx send-community extended
 exit address-family
! You need to configure your peer BGP neighbor.
```

## Configuring the Customer Site for Hierarchical VPNs: Examples

This section contains the following configuration and verification examples for the customer site:

- [Configuring PE Routers for Hierarchical VPNs: Examples, page 44](#)
- [Verifying Labels in Each PE Router for Hierarchical VPNs: Examples, page 45](#)
- [Configuring CE Routers for Hierarchical VPNs: Examples, page 47](#)
- [Verifying IP Connectivity in the Customer Site: Examples, page 47](#)

## Configuring PE Routers for Hierarchical VPNs: Examples

This example shows how to configure a PE router:

```

ip cef
!
ip vrf vpn2
 rd 200:1
  route-target export 200:1
  route-target import 200:1
mpls label protocol ldp
!
interface Loopback0
 ip address bb.bb.bb.bb 255.255.255.255
!
interface Ethernet3/0
 ip address nn.0.0.1 255.0.0.0
```

```

no ip directed-broadcast
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/3
 ip vrf forwarding vpn2
 ip address mm.0.0.2 255.0.0.0
 no ip directed-broadcast
 no ip mroute-cache
!
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 passive-interface Ethernet3/3
 network bb.bb.bb.bb 0.0.0.0 area 200
 network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 timers bgp 10 30
 neighbor hh.hh.hh.hh remote-as 200
 neighbor hh.hh.hh.hh update-source Loopback0
!
address-family vpnv4                                !VPNv4 session with PE2
 neighbor hh.hh.hh.hh activate
 neighbor hh.hh.hh.hh send-community extended
 bgp dampening 30
 exit-address-family
!
 address-family ipv4 vrf vpn2
 neighbor mm.0.0.1 remote-as 300
 neighbor mm.0.0.1 activate
 neighbor mm.0.0.1 as-override
 neighbor mm.0.0.1 advertisement-interval 5
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## Verifying Labels in Each PE Router for Hierarchical VPNs: Examples

The following examples show how to verify the configuration of PE router in hierarchical VPNs.

Verify that the loopback address of the local CE router is in the routing table of the PE1 router:

```
Router# show ip route vrf vpn2 10.2.2.2
```

```

Routing entry for 10.2.2.2/32
  Known via "bgp 200", distance 20, metric 0
  Tag 300, type external
  Last update from mm.0.0.2 20:36:59 ago
  Routing Descriptor Blocks:
  * mm.0.0.2, from mm.0.0.2, 20:36:59 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1, BGP network version 0

```

Verify that the prefix for the local CE router is in the MPLS forwarding table, and that the prefix is untagged:

```
Router# show mpls forwarding-table vrf vpn2 10.2.2.2
```



| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| 23        | Untagged           | aa.aa.aa.aa/32[V]   | 0                  | Et3/3              | nn.0.0.2 |

Verify that the prefix of the remote PE router is in the Cisco Express Forwarding table:

```
Router# show ip cef 10.5.5.5
```

```
10.5.5.5/32, version 31, cached adjacency nn.0.0.2
0 packets, 0 bytes
tag information set
  local tag: 31
  fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}
via nn.0.0.2, Ethernet3/0, 2 dependencies
  next hop nn.0.0.2, Ethernet3/0
  unresolved
  valid cached adjacency
  tag rewrite with Et3/0, nn.0.0.2, tags imposed {26}
```

Verify that the loopback address of the remote CE router is in the routing table:

```
Router# show ip route vrf vpn2 10.2.0.0
```

```
Routing entry for 10.2.0.0/32
  Known via "bgp 200", distance 200, metric 0
  Tag 300, type internal
  Last update from hh.hh.hh.hh 20:38:49 ago
  Routing Descriptor Blocks:
    * hh.hh.hh.hh (Default-IP-Routing-Table), from hh.hh.hh.hh, 20:38:49 ago
      Route metric is 0, traffic share count is 1
      AS Hops 1, BGP network version 0
```

Verify that the prefix of the remote CE router is in the MPLS forwarding table, and that an outgoing interface exists:

```
Router# show mpls forwarding-table vrf vpn2 10.2.0.0
```

| Local tag | Outgoing tag or VC | Prefix or Tunnel Id | Bytes tag switched | Outgoing interface | Next Hop |
|-----------|--------------------|---------------------|--------------------|--------------------|----------|
| None      | 26                 | jj.jj.jj.jj/32      | 0                  | Et3/0              | nn.0.0.2 |

Verify that the prefix of the remote CE router is in the Cisco Express Forwarding table:

```
Router# show ip cef vrf vpn2 10.2.0.0
```

```
10.2.0.0/32, version 12, cached adjacency nn.0.0.2
0 packets, 0 bytes
tag information set
  local tag: VPN route head
  fast tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}
via hh.hh.hh.hh, 0 dependencies, recursive
  next hop nn.0.0.2, Ethernet3/0 via hh.hh.hh.hh/32
  valid cached adjacency
  tag rewrite with Et3/0, nn.0.0.2, tags imposed {26 32}
```

Verify that the prefix of the local PE router is in the Cisco Express Forwarding table:

```
Router# show ip cef 10.1.0.0
```

```
10.1.0.0/32, version 9, connected, receive
tag information set
  local tag: implicit-null
```

## Configuring CE Routers for Hierarchical VPNs: Examples

The following example shows how to configure a CE router:

```
ip cef distributed
interface Loopback0
ip address 10.3.0.0 255.255.255.255
!
interface FastEthernet0/3/3
ip address mm.0.0.1 255.0.0.0
!
router bgp 300
no synchronization
bgp log-neighbor-changes
timers bgp 10 30
redistribute connected                                !Redistributing routes into BGP
neighbor mm.0.0.2 remote-as 200                        !to send to PE1
neighbor mm.0.0.2 advertisement-interval 5
no auto-summary
```

## Verifying IP Connectivity in the Customer Site: Examples

The following examples show how to verify IP connectivity at the customer site.

Verify that the loopback address of the remote CE router, learned from the PE router, is in the routing table of the local router:

```
Router# show ip route 10.2.0.0

Routing entry for 10.2.0.0/32
  Known via "bgp 300", distance 20, metric 0
  Tag 200, type external
  Redistributing via ospf 300
  Advertised by ospf 300 subnets
  Last update from mm.0.0.1 20:29:35 ago
  Routing Descriptor Blocks:
  * mm.0.0.1, from mm.0.0.1, 20:29:35 ago
    Route metric is 0, traffic share count is 1
    AS Hops 2
```

## Additional References

The following sections provide information related to MPLS VPNs.

## Related Documents

| Related Topic | Document Title                                   |
|---------------|--------------------------------------------------|
| LDP           | <a href="#">MPLS Label Distribution Protocol</a> |
| MPLS          | <a href="#">MPLS Product Literature</a>          |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                             |
|----------|-------------------------------------------------------------------|
| RFC 1164 | <i>Application of the Border Gateway Protocol in the Internet</i> |
| RFC 1171 | <i>A Border Gateway Protocol 4</i>                                |
| RFC 1700 | <i>Assigned Numbers</i>                                           |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i>     |
| RFC 2283 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                              |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                      |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

# Command Reference

This feature uses no new or modified commands.

# Feature Information for MPLS VPN CSC with BGP

Table 2 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 2** Feature Information for MPLS VPN CSC with BGP

| Feature Name                                                    | Releases                                                                                              | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution | 12.0(21)ST<br>12.0(22)S<br>12.0(23)S<br>12.2(13)T<br>12.0(24)S<br>12.2(14)S<br>12.0(27)S<br>12.0(29)S | This feature enables you to create an MPLS VPN CSC network that uses BGP to transport routes and MPLS labels.<br><br>In 12.0(21)ST, this feature was introduced.<br><br>In 12.0(22)S, this feature was integrated.<br><br>In 12.0(23)S, this feature was integrated.<br><br>In 12.2(13)T, this feature was integrated.<br><br>12.0(24)S, this feature was integrated.<br><br>In 12.2(14)S, this feature was integrated.<br><br>In 12.0(27)S, this feature was integrated.<br><br>In 12.0(29)S, this feature was integrated. |

# Glossary

**ASBR**—Autonomous System Boundary router. A router that connects one autonomous system to another.

**BGP**—Border Gateway Protocol. An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. In this document, the CE router sits on the edge of the customer carrier network.

**edge router**—A router that is at the edge of the network. It defines the boundary of the MPLS network. It receives and transmits packets. Also referred to as edge label switch router and label edge router.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**PE router**—provider edge router. A router, at the edge of a service provider's network, that interfaces to CE routers.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2005—2009 Cisco Systems, Inc. All rights reserved.





# Load Sharing MPLS VPN Traffic

---

**First Published: May 2, 2005**

**Last Updated: February 18, 2009**

Load sharing distributes traffic so that no individual router is overburdened. In a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) network, you can achieve load sharing through the following methods:

- BGP multipath options
- Directly connected loopback peering

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Load Sharing MPLS VPN Traffic”](#) section on page 50.

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

## Contents

- [Prerequisites for Load Sharing MPLS VPN Traffic, page 2](#)
- [Restrictions for Load Sharing MPLS VPN Traffic, page 2](#)
- [Information About Load Sharing MPLS VPN Traffic, page 4](#)
- [How to Configure Load Sharing, page 7](#)
- [Configuration Examples for Load Sharing MPLS VPN Traffic, page 46](#)
- [Additional References, page 48](#)



---

**Americas Headquarters:**

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



- [Command Reference, page 49](#)
- [Feature Information for Load Sharing MPLS VPN Traffic, page 50](#)

## Prerequisites for Load Sharing MPLS VPN Traffic

Before configuring load sharing, ensure that your MPLS VPN network (including MPLS VPN carrier supporting carrier or interautonomous system) is configured and working properly. See the “[Related Documents](#)” section on [page 48](#) for references related to MPLS VPNs.

## Restrictions for Load Sharing MPLS VPN Traffic

When you configure static routes in an MPLS or MPLS VPN environment, some variations of the **ip route** and **ip route vrf** commands are not supported. These variations of the commands are not supported in Cisco IOS releases that support the Tag Forwarding Information Base (TFIB), specifically Cisco IOS Releases 12.*n*T, 12.*n*M, and 12.0S. The TFIB cannot resolve prefixes when the recursive route over which the prefixes travel disappears and then reappears. However, the command variations are supported in Cisco IOS releases that support the MPLS Forwarding Infrastructure (MFI), specifically Cisco IOS Release 12.2(25)S and later releases. Use the following guidelines when configuring static routes.

### Supported Static Routes in an MPLS Environment

The following **ip route** command is supported when you configure static routes in an MPLS environment:

**ip route** *destination-prefix mask interface next-hop-address*

The following **ip route** commands are supported when you configure static routes in an MPLS environment and configure load sharing with static nonrecursive routes and a specific outbound interface:

**ip route** *destination-prefix mask interface1 next-hop1*  
**ip route** *destination-prefix mask interface2 next-hop2*

### Unsupported Static Routes in an MPLS Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS environment:

**ip route** *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment and enable load sharing where the next hop can be reached through two paths:

**ip route** *destination-prefix mask next-hop-address*

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment and enable load sharing where the destination can be reached through two next hops:

**ip route** *destination-prefix mask next-hop1*  
**ip route** *destination-prefix mask next-hop2*

Use the *interface* and *next-hop* arguments when specifying static routes.

### Supported Static Routes in an MPLS VPN Environment

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are associated with the same virtual routing and forwarding (VRF) instance:

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*
- **ip route vrf** *vrf-name destination-prefix mask interface1 next-hop1*  
**ip route vrf** *vrf-name destination-prefix mask interface2 next-hop2*

The following **ip route vrf** commands are supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table in the MPLS cloud in the global routing table. For example, these commands are supported when the next hop is pointing to the internet gateway.

- **ip route vrf** *vrf-name destination-prefix mask next-hop-address global*
- **ip route vrf** *vrf-name destination-prefix mask interface next-hop-address*  
(This command is supported when the next hop and the interface are in the core.)

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment and enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 next-hop1
ip route destination-prefix mask interface2 next-hop2
```

### Unsupported Static Routes in an MPLS VPN Environment That Uses the TFIB

The following **ip route** command is not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the next hop can be reached through two paths:

```
ip route vrf destination-prefix mask next-hop-address global
```

The following **ip route** commands are not supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table in the MPLS cloud within the core, and you enable load sharing where the destination can be reached through two next hops:

```
ip route vrf destination-prefix mask next-hop1 global
ip route vrf destination-prefix mask next-hop2 global
```

The following **ip route vrf** commands are not supported when you configure static routes in an MPLS VPN environment, and the next hop and interface are in the same VRF:

```
ip route vrf vrf-name destination-prefix mask next-hop1
ip route vrf vrf-name destination-prefix mask next-hop2
```

### Supported Static Routes in an MPLS VPN Environment Where the Next Hop Resides in the Global Table on the CE Router

The following **ip route vrf** command is supported when you configure static routes in an MPLS VPN environment, and the next hop is in the global table on the customer edge (CE) side. For example, the following command is supported when the destination-prefix is the CE router's loopback address, as in EBGp multihop cases.

```
ip route vrf vrf-name destination-prefix mask interface next-hop-address
```

The following **ip route** commands are supported when you configure static routes in an MPLS VPN environment, the next hop is in the global table on the CE side, and you enable load sharing with static nonrecursive routes and a specific outbound interfaces:

```
ip route destination-prefix mask interface1 nexthop1
ip route destination-prefix mask interface2 nexthop2
```

# Information About Load Sharing MPLS VPN Traffic

Before configuring load sharing features, you should understand the following concepts:

- [Load Sharing Using BGP Multipath Options, page 4](#)
- [Load Sharing Using Directly Connected Loopback Peering, page 6](#)

## Load Sharing Using BGP Multipath Options

A variety of Border Gateway Protocol (BGP) multipath options exist that enable you to configure load sharing on your MPLS VPN that uses BGP. The following sections describe some BGP multipath options:

- [Internal BGP Multipath Load Sharing, page 4](#)
- [BGP Multipath for eBGP and iBGP, page 4](#)
- [eBGP Multipath Load Sharing, page 6](#)

### Internal BGP Multipath Load Sharing

When a BGP-speaking router with no local policy configured receives multiple network layer reachability information (NLRI) from the internal BGP (iBGP) for the same destination, the router chooses one iBGP path as the best path. The best path is then installed in the IP routing table of the router. The iBGP multipath feature enables the BGP-speaking router to select multiple iBGP paths as the best paths to a destination. The best paths are then installed in the IP routing table of the router. To enable iBGP multipath load sharing, you issue the **maximum-paths ibgp** command in router configuration mode. For more information about iBGP multipath load sharing, see [Configuring BGP](#).

### BGP Multipath for eBGP and iBGP

The BGP multipath load sharing for both eBGP and iBGP in an MPLS VPN feature allows multihomed autonomous systems and provider edge (PE) routers to be configured to distribute traffic across both external BGP (eBGP) and iBGP paths.

BGP installs up to the maximum number of paths allowed (configured using the **maximum-paths** command). BGP uses the best path algorithm to select one multipath as the best path, inserts the best path into the routing information base (RIB), and advertises the best path to BGP peers. Other multipaths can be inserted into the RIB, but only one path is selected as the best path.

Cisco Express Forwarding uses multipaths to perform load balancing on a per-packet or per-source or destination pair basis. To enable the load sharing feature, configure the router with MPLS VPNs that contain VPN routing and forwarding instances (VRFs) that import both eBGP and iBGP paths. You can configure the number of multipaths separately for each VRF.

**Note**

---

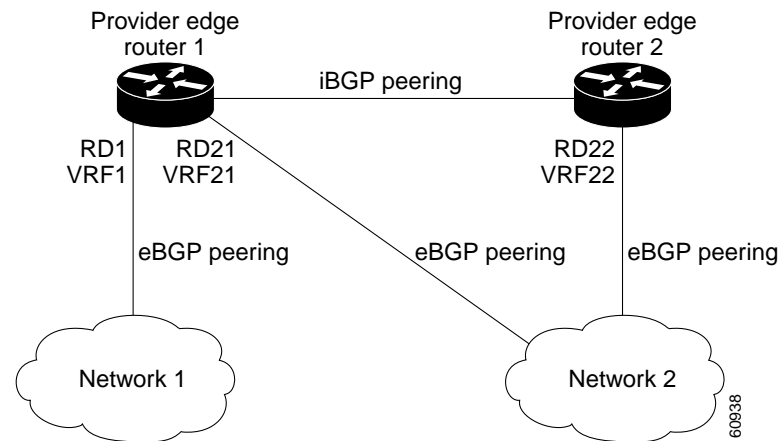
This feature operates within the configuration parameters of the existing outbound routing policy.

---

## eBGP and iBGP Multipath Load Sharing in an MPLS Network Using BGP

Figure 1 shows an MPLS service provider network using BGP that connects two remote networks to PE1 and PE2, which are both configured for VPNv4 unicast iBGP peering. Network 2 is a multihomed network that is connected to PE1 and PE2. Network 2 also has extranet VPN services configured with Network 1. Both Network 1 and Network 2 are configured for eBGP peering with the PE routers.

**Figure 1** A Service Provider MPLS Network Using BGP



You can configure PE1 so that both iBGP and eBGP paths can be selected as multipaths and imported into the VRF of Network 1. Cisco Express Forwarding uses the mutlipaths to perform load balancing. Traffic is distributed as follows:

- IP traffic that is sent from Network 2 to PE1 and PE2 is sent across the eBGP paths as IP traffic.
- IP traffic that is sent from PE1 to PE2 is sent across the iBGP path as MPLS traffic.
- MPLS traffic that is sent across an eBGP path is sent as IP traffic.

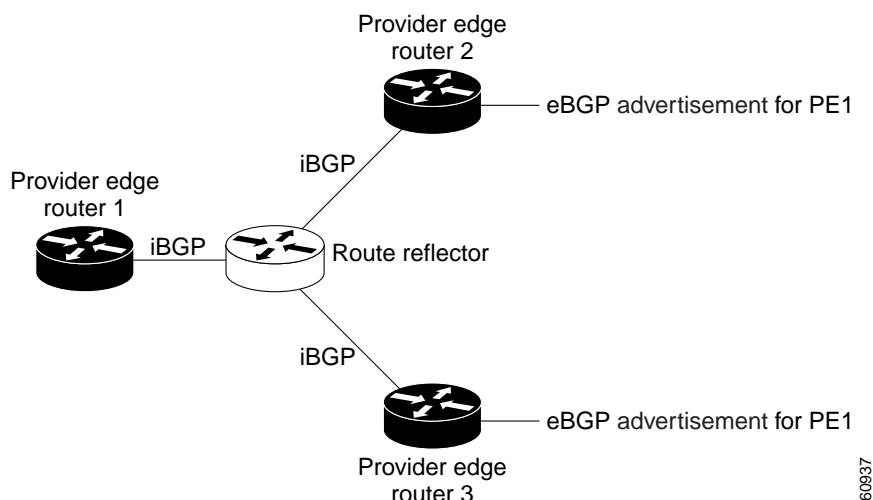
Any prefix that is advertised from Network 2 will be received by PE1 through route distinguisher (RD) 21 and RD22.

- The advertisement through RD21 is carried in IP packets.
- The advertisement through RD22 is carried in MPLS packets.

Both paths can be selected as multipaths for VRF1 and inserted into the VRF1 RIB.

## eBGP and iBGP Multipath Load Sharing with Route Reflectors

Figure 2 shows a topology that contains three PE routers and a route reflector, all configured for iBGP peering. PE2 and PE3 each advertise an equal preference eBGP path to PE1. By default, the route reflector chooses only one path and advertises PE1.

**Figure 2** *Topology with a Route Reflector*

For all equal preference paths to PE1 to be advertised through the route reflector, you must configure each VRF with a different RD. The prefixes received by the route reflector are recognized differently and advertised to PE1.

## eBGP Multipath Load Sharing

When a router learns two identical eBGP paths for a prefix from a neighboring autonomous system, it chooses the path with the lower route ID as the best path. This best path is installed in the IP routing table. You can enable eBGP multipath, which installs multiple paths in the IP routing table when the eBGP paths are learned from a neighboring autonomous system, instead of picking one best path.

During packet switching, depending on the switching mode, either per-packet or per-destination load sharing is performed among the multiple paths. The **maximum-paths** router configuration command controls the number of paths allowed. By default, BGP installs only one path to the IP routing table.

## Load Sharing Using Directly Connected Loopback Peering

You use this feature with MPLS VPN Inter-AS and MPLS VPN carrier supporting carrier (CSC) networks to load share traffic between adjacent label switched routers (LSRs) that are connected by multiple links. The LSRs could be a pair of autonomous system boundary routers (ASBRs) or a CSC-PE and a CSC-CE.

Using directly connected loopback peering allows load sharing at the IGP level, so more than one BGP session is not needed between the LSRs. No other label distribution mechanism is needed between the adjacent LSRs than BGP.

Directly connected loopback peering enables load sharing of traffic as follows:

- A BGP session is established, using the loopback addresses of the LSRs.
- MPLS is enabled on the connecting links.
- Multiple static routes to the loopback address of the adjacent LSR allow IGP load sharing.
- The outgoing label to the loopback address of the adjacent LSR is an implicit null label and is inferred by the LSR.

- Because IGP load sharing is enabled on the loopback address of the adjacent LSR, any traffic destined to a prefix that is learned over the BGP session (and recurses over the loopback) is load shared.

## How to Configure Load Sharing

This section contains the following procedures:

- [Configuring BGP Multipath Load Sharing for eBGP and iBGP, page 7](#) (required)
- [Verifying BGP Multipath Load Sharing for eBGP and iBGP, page 8](#) (optional)
- [Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS, page 9](#) (required)
- [Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier, page 11](#) (required)
- [Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses, page 16](#) (required)
- [Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS Using ASBRs to Exchange IPv4 Routes and Labels, page 23](#) (required)
- [Configuring Directly Connected Loopback Peering on MPLS VPN Carrier Supporting Carrier, page 31](#) (required)

## Configuring BGP Multipath Load Sharing for eBGP and iBGP

This section lists restrictions for load sharing.

### Restrictions

- Configuring BGP multipath for eBGP and iBGP is only for basic MPLS Layer 3 VPNs. MPLS VPN Inter-AS and MPLS VPN carrier supporting carrier do not support this multipath configuration.
- With multiple iBGP paths installed in a routing table, a route reflector advertises only one of the paths (one next hop). If a router is behind a route reflector, all routers that are connected to multihomed sites are not advertised unless separate VRFs with different RDs are configured for each VRF.
- Each IP routing table entry for a BGP prefix that has multiple iBGP paths uses additional memory. We recommend not using this feature on a router with a low amount of available memory and especially when the router is carrying a full Internet routing table.

To configure iBGP and eBGP routes for multipath load sharing, perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
5. **maximum-paths eibgp** *number-of-paths*

## DETAILED STEPS

|        | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 1                                                            | Enters router configuration mode and configures the router to run a BGP routing process.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 4 | <b>address-family ipv4 [multicast   unicast   vrf vrf-name]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vrf1 | Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes.<br><br><b>Note</b> For this task you must create the VRF and specify the <b>vrf</b> keyword. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>maximum-paths eibgp number-of-paths</b><br><br><b>Example:</b><br>Router(config-router-af)# maximum-paths eibgp 6                          | Configures the number of parallel iBGP and eBGP routes that can be installed into a routing table.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

## Verifying BGP Multipath Load Sharing for eBGP and iBGP

To verify the configuration of iBGP and eBGP routes for multipath load sharing, perform this task.

## SUMMARY STEPS

- enable**
- show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [rib-failure] [ip-prefix/length [longer-prefixes]] [network-address [mask] [longer-prefixes]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                                                                                                                                                                      | (Optional) Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                          |
| Step 2 | <b>show ip bgp vpnv4 {all   rd route-distinguisher   vrf vrf-name} [rib-failure] [ip-prefix/length [longer-prefixes]] [network-address [mask] [longer-prefixes]] [cidr-only] [community] [community-list] [dampened-paths] [filter-list] [flap-statistics] [inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp] [summary] [labels]</b><br><br><b>Example:</b><br>Router# show ip bgp vpnv4 all | Displays attributes and multipaths for a specific network in an MPLS VPN. <ul style="list-style-type: none"> <li>Enter one or more keywords or arguments.</li> </ul> |

## Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS

Perform this task on the ASBRs to configure eBGP Multipath for MPLS VPN interautonomous systems with ASBRs exchanging IPv4 routes and MPLS labels.

## Restrictions

eBGP Multipath is not supported on MPLS VPN Inter-AS with ASBRs that exchange VPNv4 routes.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
6. **maximum paths** *number-paths*
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** *ip-address* **send-label**
9. **exit-address-family**
10. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                           | Configures a BGP routing process and places the router in router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                                       |
| Step 4 | <b>neighbor {<i>ip-address</i>   <i>peer-group-name</i>}</b><br><b>remote-as <i>as-number</i></b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                          |
| Step 5 | <b>address-family ipv4 [<b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i>]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4                      | Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv4 address prefixes. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf <i>vrf-name</i></b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 6 | <b>maximum-paths <i>number-paths</i></b><br><br><b>Example:</b><br>Router(config-router-af)# maximum-paths 2                                                                          | (Optional) Controls the maximum number of parallel routes an IP routing protocol can support. <ul style="list-style-type: none"> <li>The <i>number-paths</i> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                                                                                                                                                         |

|         | Command or Action                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                        |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>activate | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 8  | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>send-label                             | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                     |
| Step 9  | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                  | Exits address family configuration mode.                                                                                                                                                                                                                                       |
| Step 10 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                  | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                      |

## Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier

This section contains the following procedures:

- [Configuring eBGP Multipath Load Sharing on the CSC-PE Routers, page 11](#)
- [Configuring eBGP Multipath Load Sharing on the CSC-CE Routers, page 13](#)

### Configuring eBGP Multipath Load Sharing on the CSC-PE Routers

Perform this task to configure eBGP Multipath load sharing on the CSC-PE routers that distribute BGP routes with MPLS labels.

#### SUMMARY STEPS

- enable**
- configure terminal**
- router bgp** *as-number*
- address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]
- maximum paths** *number-paths*
- neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
- neighbor** {*ip-address* | *peer-group-name*} **activate**
- neighbor** *ip-address* **as-override**

9. **neighbor *ip-address* send-label**
10. **exit-address-family**
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 3 | <b>router bgp <i>as-number</i></b><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                        | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <b><i>as-number</i></b> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                                  |
| Step 4 | <b>address-family ipv4 [<i>multicast</i>   <i>unicast</i>   <i>vrf vrf-name</i>]</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn1 | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b><i>multicast</i></b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b><i>unicast</i></b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b><i>vrf vrf-name</i></b> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |
| Step 5 | <b>maximum-paths <i>number-paths</i></b><br><br><b>Example:</b><br>Router(config-router-af)# maximum-paths 2                                                       | (Optional) Controls the maximum number of parallel routes an IP routing protocol can support. <ul style="list-style-type: none"> <li>On the CSC-PE router, this command is enabled in address family configuration mode.</li> <li>The <b><i>number-paths</i></b> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                         |

|         | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                             |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 7  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>activate                        | Enables the exchange of information with a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                  |
| Step 8  | <b>neighbor</b> <i>ip-address</i> <b>as-override</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>as-override                                                  | Configures a PE router to override the autonomous system number (ASN) of a site with the ASN of a provider. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the router that is to be overridden with the ASN provided.</li> </ul>                                                                                                 |
| Step 9  | <b>neighbor</b> <i>ip-address</i> <b>send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.0.0.1<br>send-label                                                    | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                          |
| Step 10 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                         | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                            |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config-router)# end                                                                                                                            | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                           |

## Configuring eBGP Multipath Load Sharing on the CSC-CE Routers

Perform this task to configure eBGP Multipath load sharing on the CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **maximum paths** *number-paths*
5. **address-family ipv4** [**multicast** | **unicast** | **vrf** *vrf-name*]

6. **redistribute** *protocol*
7. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
8. **neighbor** {*ip-address* | *peer-group-name*} **activate**
9. **neighbor** *ip-address* **send-label**
10. **exit-address-family**
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                             | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                        | Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li> </ul>                           |
| Step 4 | <b>maximum-paths</b> <i>number-paths</i><br><br><b>Example:</b><br>Router(config-router)# maximum-paths 2                                                          | (Optional) Controls the maximum number of parallel routes an IP routing protocol can support. <ul style="list-style-type: none"> <li>On the CSC-CE routers, this command is issued in router configuration mode.</li> <li>The <i>number-paths</i> argument specifies the maximum number of parallel routes an IP routing protocol installs in a routing table.</li> </ul>                                                                                          |
| Step 5 | <b>address-family ipv4</b> [ <b>multicast</b>   <b>unicast</b>   <b>vrf</b> <i>vrf-name</i> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 | Specifies the IPv4 address family type and enters address family configuration mode. <ul style="list-style-type: none"> <li>The <b>multicast</b> keyword specifies IPv4 multicast address prefixes.</li> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of the VRF to associate with subsequent IPv4 address family configuration mode commands.</li> </ul> |

|         | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6  | <p><b>redistribute</b> <i>protocol</i></p> <p><b>Example:</b><br/>Router(config-router-af)# redistribute static</p>                                                                                | <p>Redistributes routes from one routing domain into another routing domain.</p> <ul style="list-style-type: none"> <li>The <i>protocol</i> argument specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b>, <b>connected</b>, <b>egp</b>, <b>igrp</b>, <b>isis</b>, <b>mobile</b>, <b>ospf</b>, <b>rip</b>, and <b>static [ip]</b>. <ul style="list-style-type: none"> <li>The <b>static [ip]</b> keyword redistributes IP static routes.</li> </ul> </li> </ul> <p><b>Note</b> The optional <b>ip</b> keyword is used when you redistribute static routes into Intermediate System-to-Intermediate System (IS-IS).</p> <ul style="list-style-type: none"> <li>The <b>connected</b> keyword refers to routes that are established automatically when IP is enabled on an interface.</li> <li>For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes are redistributed as external to the autonomous system.</li> </ul> |
| Step 7  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>remote-as 100</p> | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 8  | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>activate</p>                        | <p>Enables the exchange of information with a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 9  | <p><b>neighbor</b> <i>ip-address</i> <b>send-label</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.0.0.2<br/>send-label</p>                                                   | <p>Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 10 | <p><b>exit-address-family</b></p> <p><b>Example:</b><br/>Router(config-router-af)# exit-address-family</p>                                                                                         | <p>Exits address family configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 11 | <p><b>end</b></p> <p><b>Example:</b><br/>Router(config-router)# end</p>                                                                                                                            | <p>(Optional) Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

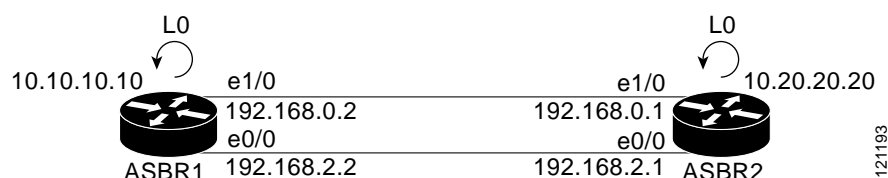
## Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses

This section describes the following tasks you need to do to configure peering of loopback interfaces of directly connected ASBRs:

- [Configuring Loopback Interface Addresses for Directly Connected ASBRs, page 16](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback, page 17](#) (required)
- [Configuring Forwarding on Connecting Loopback Interfaces, page 18](#) (required)
- [Configuring an eBGP Session Between the Loopbacks, page 19](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 22](#) (optional)

Figure 3 shows the loopback configuration for directly connected ASBR1 and ASBR2. This configuration is used as the example in the tasks that follow.

**Figure 3** Loopback Interface Configuration for Directly Connected ASBR1 and ASBR2



### Configuring Loopback Interface Addresses for Directly Connected ASBRs

Perform this task to configure loopback interface addresses for directly connected ASBRs.



#### Note

Loopback addresses need to be configured for each directly connected ASBR. That is, configure a loopback address for ASBR1 and for ASBR2 in the example shown in [Figure 3](#).

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                                  | Configures a software-only virtual interface that emulates an interface that is always up and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                           |
| Step 4 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.10.10.10 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                                       | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback

Perform this task to configure /32 static routes to the eBGP neighbor loopback.

**Note**

You need to configure /32 static routes on each of the directly connected ASBRs.

## SUMMARY STEPS

- enable**
- configure terminal**
- ip route** *prefix mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [*name*] [**permanent**] [**tag tag**]
- end**



## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                         | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <b>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]</b><br><br><b>Example:</b><br>Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1 | Establishes static routes. <ul style="list-style-type: none"> <li>The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>The <i>mask</i> argument is the prefix mask for the destination.</li> <li>The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the specified network.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>The <i>distance</i> argument is an administrative distance.</li> <li>The <i>name</i> argument applies a name to the specified route.</li> <li>The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution through the use of route maps.</li> </ul> |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                               | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring Forwarding on Connecting Loopback Interfaces

Perform this task to configure forwarding on the connecting loopback interfaces.

This task is required for sessions between loopbacks. In the [“Configuring /32 Static Routes to the eBGP Neighbor Loopback”](#) task, Ethernet 1/0 and Ethernet 0/0 are the connecting interfaces.

## SUMMARY STEPS

- enable**
- configure terminal**
- interface type slot/port**

4. **mpls bgp forwarding**
5. **exit**
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                           | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>interface type slot/port</b><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/0 | Configures an interface type and enters interface configuration mode.<br><ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>/port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp forwarding      | Configures BGP to enable MPLS forwarding on connecting interfaces.                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                    | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                            | —                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                         | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Configuring an eBGP Session Between the Loopbacks

Perform this task to configure an eBGP session between the loopbacks.

**Note**

You need to configure an eBGP session between loopbacks on each directly connected ASBR.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **no bgp default route-target filter**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family vpnv4** [**unicast**]
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
11. **end**

**DETAILED STEPS**

|        | Command or Action                                                     | Purpose                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                                         | Enables privileged EXEC mode.                                                                                                                                                                                      |
|        | <b>Example:</b><br>Router> enable                                     | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                 |
| Step 2 | <b>configure terminal</b>                                             | Enters global configuration mode.                                                                                                                                                                                  |
|        | <b>Example:</b><br>Router# configure terminal                         |                                                                                                                                                                                                                    |
| Step 3 | <b>router bgp</b> <i>as-number</i>                                    | Configures the BGP routing process.                                                                                                                                                                                |
|        | <b>Example:</b><br>Router(config)# router bgp 200                     | <ul style="list-style-type: none"> <li>The <i>as-number</i> indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul> |
| Step 4 | <b>no bgp default route-target filter</b>                             | Disables BGP route-target filtering, and enters router configuration mode.                                                                                                                                         |
|        | <b>Example:</b><br>Router(config)# no bgp default route-target filter | <ul style="list-style-type: none"> <li>All received BGP VPN-IPv4 routes are accepted by the router.</li> </ul>                                                                                                     |

|        | Command or Action                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>remote-as</b> <i>as-number</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20<br/>remote-as 100</p>                                                               | <p>Adds an entry to the BGP or multiprotocol BGP neighbor table.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                                                                                                                                               |
| Step 6 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>}<br/><b>disable-connected-check</b></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20<br/>disable-connected-check</p>                                                        | <p>Allows peering between loopbacks.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 7 | <p><b>neighbor</b> {<i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i>} <b>update-source</b> <i>interface-type</i> <i>interface-number</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.20.20.20<br/>update-source Loopback 0</p> | <p>Allows BGP sessions to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| Step 8 | <p><b>address-family</b> <b>vpn</b>v4 [<b>unicast</b>]</p> <p><b>Example:</b><br/>Router(config-router)# address-family vpnv4</p>                                                                                                                                | <p>Enters address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing.</p> <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 9 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.20.20.20<br/>activate</p>                                                                 | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p><b>Note</b> This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                              |

|         | Command or Action                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>send-community</b> [ <b>both</b>   <b>standard</b>   <b>extended</b> ]<br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.20.20.20<br>send-community extended | Specifies that a communities attribute should be sent to a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <b>both</b> keyword specifies that both standard and extended communities will be sent.</li> <li>The <b>standard</b> keyword specifies that only standard communities will be sent.</li> <li>The <b>extended</b> keyword specifies that only extended communities will be sent.</li> </ul> |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                                        | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Verifying That Load Sharing Occurs Between Loopbacks

Perform this task to verify that load sharing occurs between loopbacks. You need to ensure that the MPLS Label Forwarding Information Base (LFIB) entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]
3. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                         | Purpose                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                    | (Optional) Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                 |
| Step 2 | <b>show mpls forwarding-table</b> [ <i>network {mask   length}</i> ]   <b>labels</b> <i>label [-label]</i>   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>detail</b> ] | Displays the contents of the MPLS LFIB.<br><ul style="list-style-type: none"> <li>Enter an optional keyword or argument if desired.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                  | Exits to user EXEC mode.                                                                                                                       |

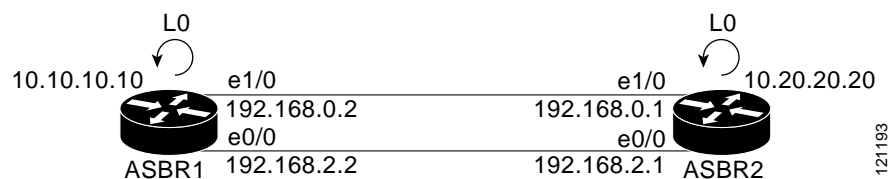
## Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS Using ASBRs to Exchange IPv4 Routes and Labels

The following sections describe how to configure peering of loopback interfaces of directly connected ASBRs to achieve load sharing in an interautonomous system network:

- [Configuring Loopback Interface Addresses for Directly Connected ASBRs, page 24](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback, page 25](#) (required)
- [Configuring Forwarding on Connecting Loopback Interfaces, page 26](#) (required)
- [Configuring an eBGP Session Between the Loopbacks, page 27](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 30](#) (optional)

Figure 4 shows the loopback configuration for directly connected ASBR1 and ASBR2. This configuration is used as the example in the tasks that follow.

**Figure 4** Loopback Interface Configuration for Directly Connected ASBR1 and ASBR2



## Configuring Loopback Interface Addresses for Directly Connected ASBRs

Perform this task to configure loopback interface addresses.



### Note

Loopback addresses need to be configured for each directly connected ASBR. That is, configure a loopback address for ASBR1 and for ASBR2 in the example shown in [Figure 4](#).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask* [secondary]
5. **end**

### DETAILED STEPS

|        | Command or Action                                       | Purpose                                                                                                                                                                                                                                          |
|--------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                 |
|        | <b>Example:</b><br>Router> enable                       |                                                                                                                                                                                                                                                  |
| Step 2 | <b>configure terminal</b>                               | Enters global configuration mode.                                                                                                                                                                                                                |
|        | <b>Example:</b><br>Router# configure terminal           |                                                                                                                                                                                                                                                  |
| Step 3 | <b>interface loopback</b> <i>interface-number</i>       | Configures a software-only virtual interface that emulates an interface that is always up and enters interface configuration mode.                                                                                                               |
|        | <b>Example:</b><br>Router(config)# interface loopback 0 | <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul> |

|        | Command or Action                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <code>ip address ip-address mask [secondary]</code><br><br><b>Example:</b><br><pre>Router(config-if)# ip address 10.10.10.10 255.255.255.255</pre> | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <code>end</code><br><br><b>Example:</b><br><pre>Router(config-if)# end</pre>                                                                       | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback

Perform this task to configure /32 static routes to the eBGP neighbor loopback.



### Note

You need to configure /32 static routes on each of the directly connected ASBRs.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask {ip-address | interface-type interface-number [ip-address]}* [*distance*] [*name*] [**permanent**] [**tag tag**]
4. **end**

## DETAILED STEPS

|        | Command or Action                                                                               | Purpose                                                                                                          |
|--------|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><pre>Router&gt; enable</pre>                      | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><pre>Router# configure terminal</pre> | Enters global configuration mode.                                                                                |



|        | Command or Action                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]</pre> <p><b>Example:</b></p> <pre>Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1</pre> | <p>Establishes static routes.</p> <ul style="list-style-type: none"> <li>The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>The <i>mask</i> argument is the prefix mask for the destination.</li> <li>The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the specified network.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>The <i>distance</i> argument is an administrative distance.</li> <li>The <i>name</i> argument applies a name to the specified route.</li> <li>The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution through the use of route maps.</li> </ul> |
| Step 4 | <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end</pre>                                                                                                                                                                               | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## Configuring Forwarding on Connecting Loopback Interfaces

Perform this task to configure forwarding on the connecting loopback interfaces.

This task is required for sessions between loopbacks. In the [“Configuring /32 Static Routes to the eBGP Neighbor Loopback”](#) task, Ethernet1/0 and Ethernet0/0 are the connecting interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot/port*
4. **mpls bgp forwarding**
5. **exit**
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0)
7. **end**

## DETAILED STEPS

|        | Command or Action                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|---------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                         |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                          | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 3 | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/0 | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>/port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp forwarding             | Configures BGP to enable MPLS forwarding on connecting interfaces.                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 5 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                           | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                                   | —                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Configuring an eBGP Session Between the Loopbacks

Perform the following tasks to configure an eBGP session between the loopbacks.

**Note**

You need to configure an eBGP session between loopbacks on each directly connected ASBR.

## SUMMARY STEPS

1. enable

2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family ipv4** [**unicast**] **vrf** *vrf-name*
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
11. **end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                          | Configures the BGP routing process, and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                        |
| Step 4 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                            | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20 remote-as 100 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the number of the autonomous system to which the neighbor belongs.</li> </ul> |

|        | Command or Action                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>disable-connected-check</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>disable-connected-check                                                         | Allows peering between loopbacks. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 7 | <b>neighbor</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i> <i>interface-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>update-source Loopback 0 | Allows BGP sessions to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p><b>Note</b> This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| Step 8 | <b>address-family</b> <b>ipv4</b> [ <b>unicast</b> ] <b>vrf</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4                                                                                                      | Enters address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of a VPN routing/forwarding instance (VRF) to associate with submodule commands.</li> </ul>                                                                                                                                                                                                                                                                                                                  |
| Step 9 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i> } <b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.20.20.20<br>activate                                                                 | Enables the exchange of information with a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p><b>Note</b> This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                                        |

|         | Command or Action                                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 10 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>send-community</b> [ <b>both</b>   <b>standard</b>   <b>extended</b> ]<br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.20.20.20<br>send-community extended | Specifies that a communities attribute should be sent to a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <b>both</b> keyword specifies that both standard and extended communities will be sent.</li> <li>The <b>standard</b> keyword specifies that only standard communities will be sent.</li> <li>The <b>extended</b> keyword specifies that only extended communities will be sent.</li> </ul> |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                                        | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Verifying That Load Sharing Occurs Between Loopbacks

To verify that load sharing can occur between loopbacks, ensure that the MPLS LFIB entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [-*label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]] [**vrf** *vrf-name*] [**detail**]
3. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                         | Purpose                                                                                                                            |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                    | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                   |
| Step 2 | <b>show mpls forwarding-table</b> [ <i>network {mask   length}</i> ]   <b>labels</b> <i>label [-label]</i>   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ] [ <b>vrf</b> <i>vrf-name</i> ] [ <b>detail</b> ] | Displays the contents of the MPLS LFIB. <ul style="list-style-type: none"> <li>Enter a keyword or argument, if desired.</li> </ul> |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                                                                                                                  | Exits to user EXEC mode.                                                                                                           |

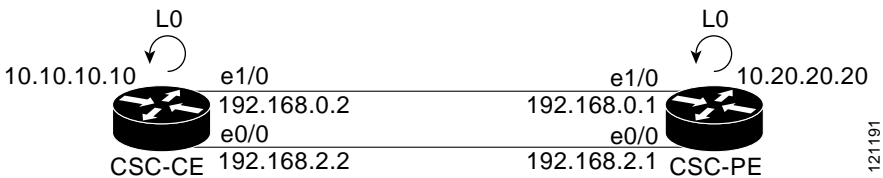
## Configuring Directly Connected Loopback Peering on MPLS VPN Carrier Supporting Carrier

The following sections explain how to load balance CSC traffic by peering loopback interfaces of directly connected CSC-PE and CSC-CE routers:

- [Configuring Loopback Interface Addresses on CSC-PE Routers, page 32](#) (required)
- [Configuring Loopback Interface Addresses for CSC-CE Routers, page 33](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-PE Router, page 34](#) (required)
- [Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-CE Router, page 36](#) (required)
- [Configuring Forwarding on CSC-PE Interfaces That Connect to the CSC-CE Loopback, page 37](#) (required)
- [Configuring Forwarding on CSC-CE Interfaces That Connect to the CSC-PE Loopback, page 39](#) (required)
- [Configuring an eBGP Session Between the CSC-PE Router and the CSC-CE Loopback, page 40](#) (required)
- [Configuring an eBGP Session Between the CSC-CE Router and the CSC-PE Loopback, page 43](#) (required)
- [Verifying That Load Sharing Occurs Between Loopbacks, page 45](#) (optional)

Figure 5 shows the loopback configuration for directly connected CSC-PE and CSC-CE routers. This configuration is used as the example in the tasks that follow.

Figure 5 Loopback Interface Configuration for Directly Connected CSC-PE and CSC-CE Routers



Restrictions

Load sharing using directly connected loopback peering does not apply to CSC networks that use LDP and an IGP to distribute routes and MPLS labels.

Configuring Loopback Interface Addresses on CSC-PE Routers

Perform this task to configure loopback interface addresses on the CSC-PE router.



Note

Configuration of a loopback interface address on the CSC-PE router requires the enabling of a VRF. The CSC-CE router loopback interface does not require the enabling a of VRF.

SUMMARY STEPS

- 1. enable
- 2. configure terminal
- 3. interface loopback *interface-number*
- 4. ip vrf forwarding *vrf-name*
- 5. ip address *ip-address mask* [secondary]
- 6. end

DETAILED STEPS

|        | Command or Action                                                                    | Purpose                                                                                                          |
|--------|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.                                                                                |

|        | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>interface loopback</b> <i>interface-number</i><br><br><b>Example:</b><br>Router(config)# interface loopback 0                                  | Configures a software-only virtual interface that emulates an interface that is always up, and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                          |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1                                      | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                  |
| Step 5 | <b>ip address</b> <i>ip-address mask</i> [ <b>secondary</b> ]<br><br><b>Example:</b><br>Router(config-if)# ip address 10.20.20.20 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                          | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring Loopback Interface Addresses for CSC-CE Routers

Perform this task to configure loopback interface addresses for CSC-CE routers.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *interface-number*
4. **ip address** *ip-address mask* [**secondary**]
5. **end**



## DETAILED STEPS

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                              |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 3 | <b>interface loopback interface-number</b><br><br><b>Example:</b><br>Router(config)# interface loopback 0                         | Configures a software-only virtual interface that emulates an interface that is always up. <ul style="list-style-type: none"> <li>The <i>interface-number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.</li> </ul>                                                                                   |
| Step 4 | <b>ip address ip-address mask [secondary]</b><br><br><b>Example:</b><br>Router(config-if)# ip address 10.10.10.10 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                                       | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-PE Router

Perform the following task to configure /32 static routes to the eBGP neighbor loopback on the CSC-PE router.

## SUMMARY STEPS

- enable**
- configure terminal**
- ip route vrf vrf-name prefix mask {ip-address | interface-type interface-number [ip-address]} [global] [distance] [name] [permanent] [tag tag]**
- end**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 3 | <b>ip route vrf vrf-name prefix mask {ip-address   interface-type interface-number [ip-address]} [global] [distance] [name] [permanent] [tag tag]</b><br><br><b>Example:</b><br>Router(config)# ip route vrf vpn1 10.10.10.10 255.255.255.255 Ethernet 1/0 172.16.0.2 | Establishes static routes for a VRF. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name of the VRF for the static route.</li> <li>The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>The <i>mask</i> argument is the prefix mask for the destination.</li> <li>The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the destination network.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>The <b>global</b> keyword specifies that the given next hop address is in the nonVRF routing table.</li> <li>The <i>distance</i> argument is an administrative distance.</li> <li>The <i>name</i> argument applies a name to the specified route.</li> <li>The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution via route maps.</li> </ul> |
| Step 4 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Configuring /32 Static Routes to the eBGP Neighbor Loopback on the CSC-CE Router

Perform the following task to configure /32 static routes to the eBGP neighbor loopback for the CSC-CE router.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip route** *prefix mask {ip-address | interface-type interface-number [ip-address]}* [*distance*] [*name*] [**permanent**] [**tag tag**]
4. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                                                          |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |
|        | <b>Example:</b><br>Router> enable             |                                                                                                                  |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                                                  |

|        | Command or Action                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <pre>ip route prefix mask {ip-address   interface-type interface-number [ip-address]} [distance] [name] [permanent] [tag tag]</pre> <p><b>Example:</b></p> <pre>Router(config)# ip route 10.20.20.20 255.255.255.255 Ethernet 1/0 172.16.0.1</pre> | <p>Establishes static routes.</p> <ul style="list-style-type: none"> <li>The <i>prefix</i> argument is the IP route prefix for the destination.</li> <li>The <i>mask</i> argument is the prefix mask for the destination.</li> <li>The <i>ip-address</i> argument is the IP address of the next hop that you can use to reach the destination network.</li> <li>The <i>interface-type</i> and <i>interface-number</i> arguments are the network interface type and interface number.</li> <li>The <i>distance</i> argument is an administrative distance.</li> <li>The <i>name</i> argument applies a name to the specified route.</li> <li>The <b>permanent</b> keyword specifies that the route is not to be removed, even if the interface shuts down.</li> <li>The <b>tag tag</b> keyword and argument name a tag value that can be used as a “match” value for controlling redistribution via route maps.</li> </ul> |
| Step 4 | <pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end</pre>                                                                                                                                                                               | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

## Configuring Forwarding on CSC-PE Interfaces That Connect to the CSC-CE Loopback

Perform this task to configure forwarding on CSC-PE interfaces that connect to the CSC-CE loopback.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type slot/port**
4. **ip vrf forwarding vrf-name**
5. **ip address ip-address mask [secondary]**
6. **mpls bgp forwarding**
7. **exit**
8. Repeat Steps 3 through 6 for another connecting interface (Ethernet 0/0).
9. **end**

## DETAILED STEPS—CSC-PE

|        | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface type slot/port</b><br><br><b>Example:</b><br>Router(config)# interface ethernet 1/0                                 | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument is the type of interface to be configured.</li> <li>The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>The <i>port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |
| Step 4 | <b>ip vrf forwarding vrf-name</b><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1                            | Associates a VRF with an interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                       |
| Step 5 | <b>ip address ip-address mask [secondary]</b><br><br><b>Example:</b><br>Router(config-if)# ip address 172.16.0.1 255.255.255.255 | Sets a primary or secondary IP address for an interface. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address.</li> <li>The <i>mask</i> argument is the mask for the associated IP subnet.</li> <li>The <b>secondary</b> keyword specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address.</li> </ul>                           |
| Step 6 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp forwarding                                      | Configures BGP to enable MPLS forwarding on connecting interfaces.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 7 | <b>exit</b><br><br><b>Example:</b><br>Router(config-if)# exit                                                                    | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                     |

|        | Command or Action                                                           | Purpose                        |
|--------|-----------------------------------------------------------------------------|--------------------------------|
| Step 8 | Repeat Steps 3 through 6 for another connecting interface (Ethernet 0/0).   | —                              |
| Step 9 | <code>end</code><br><br><b>Example:</b><br><code>Router(config)# end</code> | Exits to privileged EXEC mode. |

## Configuring Forwarding on CSC-CE Interfaces That Connect to the CSC-PE Loopback

Perform this task to configure forwarding on CSC-CE interfaces that connect to the CSC-PE loopback.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot/port`
4. `mpls bgp forwarding`
5. `exit`
6. Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).
7. `end`

### DETAILED STEPS

|        | Command or Action                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <code>enable</code><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <code>configure terminal</code><br><br><b>Example:</b><br><code>Router# configure terminal</code>                   | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <code>interface type slot/port</code><br><br><b>Example:</b><br><code>Router(config)# interface ethernet 1/0</code> | Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> <li>• The <i>type</i> argument is the type of interface to be configured.</li> <li>• The <i>slot</i> argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</li> <li>• The <i>/port</i> argument is the port number. Refer to the appropriate hardware manual for slot and port information.</li> </ul> |

|        | Command or Action                                                                                              | Purpose                                                            |
|--------|----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Step 4 | <code>mpls bgp forwarding</code><br><br><b>Example:</b><br><code>Router(config-if)# mpls bgp forwarding</code> | Configures BGP to enable MPLS forwarding on connecting interfaces. |
| Step 5 | <code>exit</code><br><br><b>Example:</b><br><code>Router(config-if)# exit</code>                               | Exits to global configuration mode.                                |
| Step 6 | Repeat Steps 3 and 4 for another connecting interface (Ethernet 0/0).                                          | —                                                                  |
| Step 7 | <code>end</code><br><br><b>Example:</b><br><code>Router(config)# end</code>                                    | Exits to privileged EXEC mode.                                     |

## Configuring an eBGP Session Between the CSC-PE Router and the CSC-CE Loopback

Perform this task to configure an eBGP session between the CSC-PE router and the CSC-CE loopback.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `router bgp as-number`
4. `bgp log-neighbor-changes`
5. `neighbor {ip-address | peer-group-name} remote-as as-number`
6. `neighbor {ip-address | peer-group-name} disable-connected-check`
7. `neighbor {ip-address | ipv6-address | peer-group-name} update-source interface-type interface-number`
8. `address-family ipv4 [unicast] vrf vrf-name`
9. `ip vrf forwarding vrf-name`
10. `neighbor {ip-address | peer-group-name | ipv6-address} activate`
11. `neighbor ip-address send-label`
12. `end`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                               |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                              |
| Step 3 | <b>router bgp as-number</b><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                              | Configures the BGP routing process. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                                                |
| Step 4 | <b>bgp log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                         | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                        |
| Step 5 | <b>neighbor {ip-address   peer-group-name}</b><br><b>remote-as as-number</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.10<br>remote-as 100               | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul> |
| Step 6 | <b>neighbor {ip-address   peer-group-name}</b><br><b>disable-connected-check</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.10.10.10<br>disable-connected-check | Allows peering between loopbacks. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                            |



|         | Command or Action                                                                                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7  | <p><b>neighbor</b> {<i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i>} <b>update-source</b> <i>interface-type</i> <i>interface-number</i></p> <p><b>Example:</b><br/>Router(config-router)# neighbor 10.10.10.10<br/>update-source Loopback 0</p> | <p>Allows BGP sessions to use any operational interface for TCP connections.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p> <ul style="list-style-type: none"> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |
| Step 8  | <p><b>address-family</b> <b>ipv4</b> [<b>unicast</b>] <b>vrf</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config-router)# address-family ipv4 vrf<br/>vpn1</p>                                                                                          | <p>Enters address family configuration mode for configuring routing protocols such as BGP, Routing Information Protocol (RIP), and static routing.</p> <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword configures sessions that carry standard IPv4 address prefixes.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument specify the name of a VRF to associate with submode commands.</li> </ul>                                                                                                                                                                                                                                          |
| Step 9  | <p><b>ip vrf forwarding</b> <i>vrf-name</i></p> <p><b>Example:</b><br/>Router(config-router-af)# ip vrf forwarding<br/>vpn1</p>                                                                                                                                  | <p>Associates a VRF with an interface or subinterface.</p> <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Step 10 | <p><b>neighbor</b> {<i>ip-address</i>   <i>peer-group-name</i>   <i>ipv6-address</i>} <b>activate</b></p> <p><b>Example:</b><br/>Router(config-router-af)# neighbor 10.10.10.10<br/>activate</p>                                                                 | <p>Enables the exchange of information with a BGP neighbor.</p> <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <p><b>Note</b> This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</p>                                                                                                                                                                                            |

|         | Command or Action                                                            | Purpose                                                                                                                       |
|---------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Step 11 | <b>neighbor</b> <i>ip-address</i> <b>send-label</b>                          | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.                                         |
|         | <b>Example:</b><br>Router(config-router-af)# neighbor 10.10.10.10 send-label | <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> </ul> |
| Step 12 | <b>end</b>                                                                   | Exits to privileged EXEC mode.                                                                                                |
|         | <b>Example:</b><br>Router(config)# end                                       |                                                                                                                               |

## Configuring an eBGP Session Between the CSC-CE Router and the CSC-PE Loopback

Perform this task to configure an eBGP session between the CSC-CE router and the CSC-PE loopback.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **bgp log-neighbor-changes**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
6. **neighbor** {*ip-address* | *peer-group-name*} **disable-connected-check**
7. **neighbor** {*ip-address* | *ipv6-address* | *peer-group-name*} **update-source** *interface-type interface-number*
8. **address-family ipv4** [**unicast**] [**vrf** *vrf-name*]
9. **neighbor** {*ip-address* | *peer-group-name* | *ipv6-address*} **activate**
10. **neighbor** *ip-address* **send-label**
11. **end**

### DETAILED STEPS

|        | Command or Action                             | Purpose                                                                            |
|--------|-----------------------------------------------|------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b>                                 | Enables privileged EXEC mode.                                                      |
|        | <b>Example:</b><br>Router> enable             | <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>configure terminal</b>                     | Enters global configuration mode.                                                  |
|        | <b>Example:</b><br>Router# configure terminal |                                                                                    |

|        | Command or Action                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 3 | <b>router</b> <b>bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 200                                                                                                                                                        | Configures the BGP routing process. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 4 | <b>bgp</b> <b>log-neighbor-changes</b><br><br><b>Example:</b><br>Router(config-router)# bgp log-neighbor-changes                                                                                                                                          | Enables logging of BGP neighbor resets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 5 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>remote-as 100                                                                | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>as-number</i> argument is the autonomous system to which the neighbor belongs.</li> </ul>                                                                                                                                                                                                                                                                                                                        |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>disable-connected-check</b><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>disable-connected-check                                                         | Allows peering between loopbacks. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Step 7 | <b>neighbor</b> { <i>ip-address</i>   <i>ipv6-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i> <i>interface-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 10.20.20.20<br>update-source Loopback 0 | Allows BGP sessions to use any operational interface for TCP connections. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IPv4 address of the BGP-speaking neighbor.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.<br/><br/>This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons.</li> <li>The <i>peer-group-name</i> argument is the name of a BGP peer group.</li> <li>The <i>interface-type</i> argument is the interface type.</li> <li>The <i>interface-number</i> argument is the interface number.</li> </ul> |

|         | Command or Action                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 8  | <b>address-family ipv4</b> [ <b>unicast</b> ] [ <b>vrf vrf-name</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family ipv4                                             | Enters address family configuration mode for configuring routing protocols such as BGP, RIP, and static routing. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword configures sessions that carry standard IPv4 address prefixes.</li> <li>The <b>unicast</b> keyword specifies unicast prefixes.</li> <li>The <b>vrf vrf-name</b> keyword and argument specify the name of a VRF to associate with submode commands.</li> </ul>                                                                              |
| Step 9  | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> / <i>ipv6-address</i> } <b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.20.20.20 activate | Enables the exchange of information with a BGP neighbor. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> <li>The <i>peer-group-name</i> argument is the name of the BGP peer group.</li> <li>The <i>ipv6-address</i> argument is the IPv6 address of the BGP-speaking neighbor.</li> </ul> <b>Note</b> This argument must be in the form documented in RFC 2373, where the address is specified in hexadecimal using 16-bit values between colons. |
| Step 10 | <b>neighbor ip-address send-label</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 10.20.20.20 send-label                                                              | Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument is the IP address of the neighboring router.</li> </ul>                                                                                                                                                                                                                                                                                                        |
| Step 11 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                               | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Verifying That Load Sharing Occurs Between Loopbacks

To verify that load sharing occurs between loopbacks, ensure that the MPLS LFIB entry for the neighbor route lists the available paths and interfaces.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table** [**vrf vrf-name**] [{*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]}] [**detail**]
3. **disable**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                | Purpose                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show mpls forwarding-table</b> [vrf vrf-name] [{network {mask   length}   labels label [- label]   interface interface   next-hop address   lsp-tunnel {tunnel-id}}] [detail] | Displays the contents of the MPLS LFIB.                                                                          |
| Step 3 | <b>disable</b><br><br><b>Example:</b><br>Router# disable                                                                                                                         | Exits to user EXEC mode.                                                                                         |

## Configuration Examples for Load Sharing MPLS VPN Traffic

This section contains the following configuration examples for Load Sharing MPLS VPN Traffic:

- [Configuring a Router to Select eBGP or iBGP Paths as Multipaths: Example, page 46](#)
- [Configuring a /32 Static Route from an ASBR to the Loopback Address of Another ASBR: Examples, page 46](#)
- [Configuring BGP/MPLS Forwarding on the Interfaces Connecting ASBRs: Example, page 47](#)
- [Configuring VPNv4 Sessions on an ASBR: Example, page 47](#)
- [Verifying VPN NLRI for a Specified Network: Example, page 47](#)

### Configuring a Router to Select eBGP or iBGP Paths as Multipaths: Example

The following example configures a router in address family configuration mode to select six eBGP or iBGP paths as multipaths:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf try
Router(config-router-af)# maximum-paths eibgp 6
Router(config-router-af)# end
```

### Configuring a /32 Static Route from an ASBR to the Loopback Address of Another ASBR: Examples

The following example configures a /32 static route from ASBR1 to the loopback address of ASBR2:

```
Router# configure terminal
Router(config)# ip route 10.20.20.20 255.255.255 e1/0 168.192.0.1
```

```
Router(config)# ip route 10.20.20.20 255.255.255 e0/0 168.192.2.1
```

The following example configures a /32 static route from ASBR2 to the loopback address of ASBR1:

```
Router# configure terminal
Router(config)# ip route vrf vpn1 10.10.10.10 255.255.255 e1/0 168.192.0.2
Router(config)# ip route vrf vpn1 10.10.10.10 255.255.255 e0/0 168.192.2.2
```

## Configuring BGP/MPLS Forwarding on the Interfaces Connecting ASBRs: Example

The following example configures BGP/MPLS forwarding on the interfaces connecting ASBR2 with ASBR1:

```
Router# configure terminal
Router(config)# interface ethernet 1/0
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# ip address 168.192.0.1 255.255.255.255
Router(config-if)# mpls bgp forwarding
Router(config-if)# exit
Router(config)# interface ethernet 0/0
Router(config-if)# ip vrf forwarding vpn1
Router(config-if)# ip address 168.192.2.1 255.255.255.255
Router(config-if)# mpls bgp forwarding
Router(config-if)# exit
```

## Configuring VPNv4 Sessions on an ASBR: Example

The following example configures VPNv4 sessions on ASBR2:

```
Router# configure terminal
Router(config)# router bgp 200
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.10.10.10 remote-as 100
Router(config-router)# neighbor 10.10.10.10 disable-connected-check
Router(config-router)# neighbor 10.10.10.10 update-source Loopback0
!
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.10.10.10 activate
Router(config-router-af)# neighbor 10.10.10.10 send-community extended
Router(config-router-af)# end
```

## Verifying VPN NLRI for a Specified Network: Example

If you enter the **all** keyword with the **show ip bgp vpnv4** command, the output displays information about all VPN network layer reachability information (NLRI) for a specified network:

```
Router# show ip bgp vpnv4 all 10.22.22.0

BGP routing table entry for 10:1:22.22.22.0/24, version 19
Paths:(5 available, best #5)
Multipath: eiBGP
  Advertised to non peer-group peers:
    10.0.0.2 10.0.0.3 10.0.0.4 10.0.0.5
  22
    10.0.0.2 (metric 20) from 10.0.0.4 (10.0.0.4)
      Origin IGP, metric 0, localpref 100, valid, internal, multipath
```

```

Extended Community:0x0:0:0 RT:100:1 0x0:0:0
Originator:10.0.0.2, Cluster list:10.0.0.4
22
10.0.0.2 (metric 20) from 10.0.0.5 (10.0.0.5)
Origin IGP, metric 0, localpref 100, valid, internal, multipath
Extended Community:0x0:0:0 RT:100:1 0x0:0:0
Originator:10.0.0.2, Cluster list:10.0.0.5
22
10.0.0.2 (metric 20) from 10.0.0.2 (10.0.0.2)
Origin IGP, metric 0, localpref 100, valid, internal, multipath
Extended Community:RT:100:1 0x0:0:0
22
10.0.0.2 (metric 20) from 10.0.0.3 (10.0.0.3)
Origin IGP, metric 0, localpref 100, valid, internal, multipath
Extended Community:0x0:0:0 RT:100:1 0x0:0:0
Originator:10.0.0.2, Cluster list:10.0.0.3
22
10.1.1.12 from 10.1.1.12 (10.22.22.12)
Origin IGP, metric 0, localpref 100, valid, external, multipath, best
Extended Community:RT:100:1

```

## Additional References

The following sections provide references related to MPLS VPNs.

## Related Documents

| Related Topic | Document Title                                                                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| MPLS          | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 15.0, MPLS VPN Carrier Supporting Carrier with BGP</a> |
| BGP           | <a href="#">Cisco IOS IP Routing: BGP Configuration Guide, Release 15.0, Configuring BGP</a>                                            |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                             |
|----------|-------------------------------------------------------------------|
| RFC 1164 | <i>Application of the Border Gateway Protocol in the Internet</i> |
| RFC 1171 | <i>A Border Gateway Protocol 4</i>                                |
| RFC 1700 | <i>Assigned Numbers</i>                                           |
| RFC 1966 | <i>BGP Route Reflection: An Alternative to Full Mesh IBGP</i>     |
| RFC 2283 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 2373 | <i>IP Version 6 Addressing Architecture</i>                       |
| RFC 2547 | <i>BGP/MPLS VPNs</i>                                              |
| RFC 2842 | <i>Capabilities Advertisement with BGP-4</i>                      |
| RFC 2858 | <i>Multiprotocol Extensions for BGP-4</i>                         |
| RFC 3107 | <i>Carrying Label Information in BGP-4</i>                        |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

This feature uses no new or modified commands.



# Feature Information for Load Sharing MPLS VPN Traffic

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Load Sharing MPLS VPN Traffic

| Feature Name                                                     | Releases                           | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Load Balancing Support for Inter-AS and CSC VPNs        | 12.0(29)S<br>12.4(20)T             | <p>This feature allows MPLS VPN Inter-AS and MPLS VPN CSC networks to load share traffic between adjacent LSRs that are connected by multiple links. The LSRs can be a pair of ASBRs or a CSC-PE and a CSC-CE. Using directly connected loopback peering allows load sharing at the IGP level, so more than one BGP session is not needed between the LSRs. No other label distribution mechanism is needed between the adjacent LSRs than BGP.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Load Sharing Using Directly Connected Loopback Peering, page 6</a></li> <li>• <a href="#">Configuring Directly Connected Loopback Peering for MPLS VPN Inter-AS using ASBRs to Exchange VPN-IPv4 Addresses, page 16</a></li> </ul> |
| BGP Multipath Load Sharing for Both eBGP and iBGP in an MPLS VPN | 12.2(4)T<br>12.2(14)S<br>12.0(24)S | <p>This feature allows multihomed autonomous systems and PE routers to be configured to distribute traffic across both external BGP (eBGP) and internal BGP (iBGP) paths.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">BGP Multipath for eBGP and iBGP, page 4</a></li> <li>• <a href="#">Configuring BGP Multipath Load Sharing for eBGP and iBGP, page 7</a></li> </ul>                                                                                                                                                                                                                                                                                                                                                       |

**Table 1**      **Feature Information for Load Sharing MPLS VPN Traffic (continued)**

| Feature Name                | Releases              | Feature Configuration Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| iBGP Multipath Load Sharing | 12.2(2)T<br>12.2(14)S | This feature enables the BGP speaking router to select multiple iBGP paths as the best paths to a destination.<br><br>The following section provides information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">Internal BGP Multipath Load Sharing, page 4</a></li> </ul>                                                                                                                                                                                                                                                                           |
| eBGP Multipath              | 12.0(27)S             | This feature installs multiple paths in the IP routing table when the eBGP paths are learned from a neighboring Autonomous System (AS), instead of picking one best path.<br><br>The following sections provide information about this feature: <ul style="list-style-type: none"> <li>• <a href="#">eBGP Multipath Load Sharing, page 6</a></li> <li>• <a href="#">Configuring eBGP Multipath Load Sharing with MPLS VPN Inter-AS, page 9</a></li> <li>• <a href="#">Configuring eBGP Multipath Load Sharing with MPLS VPN Carrier Supporting Carrier, page 11</a></li> </ul> |

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2005–2009 Cisco Systems, Inc. All rights reserved.





# MPLS VPN—Inter-AS Option AB

---

**First Published: December 17, 2007**

**Last Updated: October 2, 2009**

The MPLS VPN—Inter-AS Option AB feature combines the best functionality of an Inter-AS Option (10) A and Inter-AS Option (10) B network to allow a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) service provider to interconnect different autonomous systems to provide VPN services. These networks are defined in RFC 4364 section 10 “Multi-AS Backbones,” option “a” and option “b” respectively.

When different autonomous systems are interconnected in an MPLS VPN—Inter-AS Option AB configuration, the entire network configuration is scaled and simplified, and maintains IP Quality of Service (QoS) functions between Autonomous System Boundary Router (ASBR) peers.

In an Inter-AS Option A network, ASBR peers are connected by multiple sub-interfaces with at least one interface VPN that spans the two autonomous systems. These ASBRs associate each sub-interface with a VRF and a BGP session to signal unlabeled IP prefixes. As a result, traffic between the back-to-back VRFs is IP. In this scenario, the VPNs are isolated from each other and because the traffic is IP, QoS mechanisms that operate on IP traffic can be applied to achieve customer Service Level Agreements (SLAs). The downside of this configuration is that there needs to be one BGP session for each sub-interface (and at least one subinterface for each VPN), which causes scalability concerns as this network grows.

In an Inter-AS Option B network, ASBR peers are connected by one or more sub-interfaces that are enabled to receive MPLS traffic. A Multi-protocol Border Gateway Protocol (MP-BGP) session is used to distribute labeled VPN prefixes between the ASBR. As a result, the traffic that flows between them is labeled. The downside of this configuration is that because the traffic is MPLS, QoS mechanisms that can only be applied to IP traffic cannot be applied and the VRFs cannot be isolated.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS VPN—Inter-AS Option AB” section on page 45](#).



---

**Americas Headquarters:**

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

**Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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

## Contents

- [Prerequisites for MPLS VPN—Inter-AS Option AB, page 2](#)
- [Restrictions for MPLS VPN—Inter-AS Option AB, page 2](#)
- [Information About MPLS VPN—Inter-AS Option AB, page 3](#)
- [How to Configure Inter-AS Option AB, page 9](#)
- [Configuration Examples for MPLS VPN—Inter-AS Option AB, page 18](#)
- [Additional References, page 42](#)
- [Feature Information for MPLS VPN—Inter-AS Option AB, page 45](#)
- [Glossary, page 46](#)

## Prerequisites for MPLS VPN—Inter-AS Option AB

Follow the appropriate configuration tasks outlined in the following documents:

- [Configuring MPLS Layer 3 VPNs](#)
- [MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses](#)
- [MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels](#)

Perform the following requirements before configuring the MPLS VPN—Inter-AS Option AB feature.

- Enable Cisco Express Forwarding, which is required for MPLS VPN routing and forwarding operation.
- Identify the VPNs for the MPLS VPN—Inter-AS Option AB network and configure the VRFs to which these VPNs belong. These VRFs are used for Inter-AS Option AB connections on the ASBR interface.

## Restrictions for MPLS VPN—Inter-AS Option AB

This feature has the following restrictions:

- The In Service Software Upgrade (ISSU) feature can only be configured on the active Route Processor (RP) if the standby RP supports this feature. The ISSU feature can be configured if both the active and standby RP support this feature.
- Carrier Supporting Carrier (CSC) MPLS load-balancing on ASBR Option AB VRF interfaces is not supported.
- VPNv6 is not supported.

# Information About MPLS VPN—Inter-AS Option AB

This section provides an introduction to the MPLS VPN—Inter-AS Option AB feature and describes its benefits:

- [MPLS VPN—Inter-AS Option AB Introduction, page 2](#)
- [Benefits of MPLS VPN—Inter-AS Option AB, page 2](#)
- [MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding in Non-CSC Networks, page 4](#)
- [MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding for CSC, page 7](#)

## MPLS VPN—Inter-AS Option AB Introduction

MPLS VPN service providers need to interconnect different autonomous systems to provide service for multiple VPN customers. The MPLS VPN—Inter-AS Option AB feature allows the different autonomous systems to interconnect by using a single MP-BGP session in the global routing table to carry control plane traffic. This MP-BGP session signals VPN prefixes between two ASBRs for each virtual routing and forwarding (VRF) instance. The data plane traffic is on a VRF interface. This traffic can either be IP or MPLS.

**Note**

Inter-AS connections can be configured between ASBRs that either have or do not have connections between different providers.

## Benefits of MPLS VPN—Inter-AS Option AB

The MPLS VPN—Inter-AS Option AB feature provides the following benefits for service providers:

- Network configuration can be simplified because only one BGP session is configured for each VRF on the ASBR.
- One BGP session reduces CPU utilization.
- Networks can be scaled because a single MP-BGP session, which is enabled globally on the router, reduces the number of sessions required by multiple VPNs, while continuing to keep VPNs isolated and secured from each other.
- IP QoS functions between ASBR peers are maintained for customer SLAs.
- Dataplane traffic is isolated on a per-VRF basis for security purposes.

## MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding in Non-CSC Networks

The following sections describe MPLS VPN—Inter-AS Option AB operation:

- [Route Distribution for VPN 1, page 5](#)
- [Packet Forwarding for VPN 1, page 5](#)
- [Route Distribution for VPN 2, page 6](#)



### Note

All imported routes are accomplished by configuring the appropriate route targets (RTs).

The following attributes describe the topology of the sample MPLS VPN—Inter-AS Option AB network shown in [Figure 1 on page 4](#):

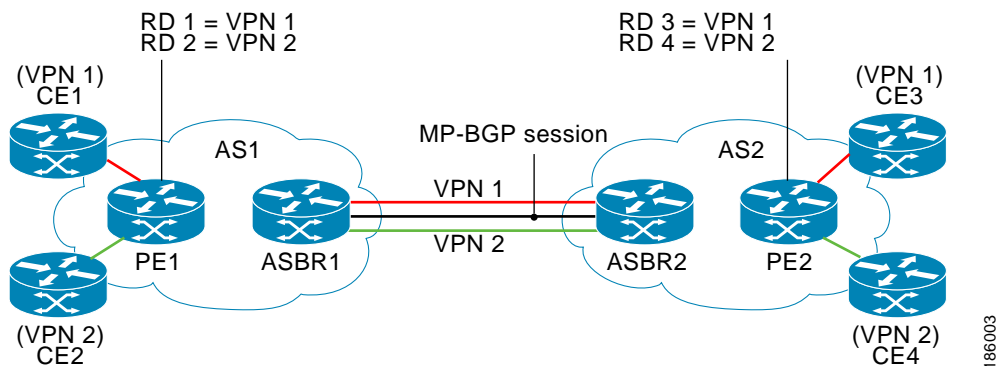
- Customer edge 1 (CE1) and CE3 belong to VPN 1.
- CE2 and CE 4 belong to VPN 2.
- Provider edge 1 (PE1) uses route distinguisher 1 (RD 1) for VPN 1 (VRF 1) and RD 2 for VPN 2 (VRF 2).
- PE2 uses RD 3 for VPN 1 (VRF 1) and RD 4 for VPN 2 (VRF 2).
- ASBR1 has VRF 1 provisioned with RD 5 and VRF 2 provisioned with RD 6.
- ASBR2 has VRF 1 provisioned with RD 7 and VRF 2 provisioned and RD 8.
- ASBR1 and ASBR2 have three links between them:
  - VRF 1
  - VRF 2
  - MP-BGP session



### Note

The VRFs configured on the ASBRs are called “Option AB VRFs.” The eBGP peers on the ASBRs are called “Option AB Peers.”

**Figure 1** *MPLS VPN Inter-AS Option AB Topology*



136003

## Route Distribution for VPN 1

A route distinguisher (RD) is an identifier attached to a route that identifies which VPN belongs to each route. Each routing instance must have a unique RD autonomous system associated with it. The RD is used to place a boundary around a VPN so that the same IP address prefixes can be used in different VPNs without having these IP address prefixes overlap.



### Note

An RD statement is required if the instance type is a VRF.

The following process describes the route distribution process for VPN 1 in [Figure 1](#). Prefix “N” is used in this process to indicate the IP address of a VPN.

1. CE1 advertises the prefix N to PE1.
2. PE1 advertises a VPN prefix RD 1:N to ASBR1 through MP internal BGP (iBGP).
3. ASBR1 imports the prefix into VPN 1 and creates a prefix RD 5:N.
4. ASBR1 advertises the imported prefix RD 5:N to ASBR2. ASBR1 sets itself as the next hop for prefix RD 5:N and allocates a local label that is signaled with this prefix.
5. ASBR1 advertises the route with the export RT configured on the VRF rather than the originally received RTs. By default, ASBR1 does not advertise the source prefix RD 1:N to ASBR2. This advertisement is suppressed because the prefix is being imported into an Option AB VRF.



### Note

In an Option 10B connection, the source prefix can be advertised to another ASBR on which ASBR1 has an Option 10B connection. An ASBR with an Option 10B connection maintains all VPNv4 routes in its BGP table.

6. ASBR2 receives the prefix RD 5:N and imports it into VPN 1 as RD 7:N.
7. ASBR2 advertises the route with the export RT configured on the VRF rather than the originally received RTs.
8. While importing the prefix, ASBR2 sets the next hop of RD 7:N to the ASBR1 interface IP address in VRF 1. The next hop table ID is also set to VRF 1. When installing the MPLS forwarding entry for RD 7:N, the outgoing label is not installed in forwarding by default. This enables the traffic between the ASBRs to be IP.
9. ASBR2 advertises the imported prefix RD 7:N to PE2. It sets itself as the next hop for this prefix and also allocates a local label that is signaled with the prefix. By default, ASBR2 does not advertise the source prefix RD 5:N to PE2. This advertisement is suppressed because the prefix is being imported into an Option AB VRF.
10. PE2 imports the RD 7:N into VRF 1 as RD 3:N.

## Packet Forwarding for VPN 1

The following packet forwarding process works the same as it does in an Option A scenario. The ASBR acts like the PE by terminating the VPN and then forwards its traffic as standard IP packets with no VPN label to the next PE, which in turn repeats the VPN process. Each PE router, therefore, treats the adjacent PE router as a CE router, and the standard Layer 3 MPLS VPN mechanisms are used for route redistribution with each autonomous system; that is, the PEs use external BGP (eBGP) to distribute unlabeled IPv4 addresses to each other.



**Note**

Prefix “N” is used in this process to indicate the IP address of a VPN.

1. CE3 sends a packet destined for N to PE2.
2. PE2 encapsulates the packet with the VPN label allocated by ASBR2 and the IGP label needed to tunnel the packet to ASBR2.
3. The packet arrives on ASBR2 with the VPN label. ASBR2 removes the VPN label and sends the packet as IP to ASBR1 on the VRF 1 interface.
4. The IP packet arrives at ASBR1 on the VRF 1 interface. ASBR1 then encapsulates the packet with the VPN label allocated by PE1 and the IGP label needed to tunnel the packet to PE1.
5. The packet arrives on PE1 with the VPN label. PE1 disposes the VPN label and forwards the IP packet to CE1.

## Route Distribution for VPN 2

The following information describes the route distribution process for VPN 2 in [Figure 1](#):

1. CE2 advertises prefix N to PE1, where N is the VPN IP address.
2. PE1 advertises a VPN prefix RD 2:N to ASBR1 through MP-iBGP.
3. ASBR1 imports the prefix into VPN 2 and creates a prefix RD 6:N.
4. ASBR1 advertises the imported prefix RD 6:N to ASBR2. It sets itself as the next hop for this prefix and also allocates a local label that is signaled with the prefix. By default, ASBR1 does not advertise the source prefix RD 2:N to ASBR2. This advertisement is suppressed as the prefix is being imported into an Option AB VRF.

**Note**

In the case of an Option 10B connection, the source prefix can be advertised to another ASBR on which ASBR1 has an Option 10B connection. An ASBR with an Option 10B connection maintains all VPNv4 routes in its BGP table.

5. ASBR2 receives the prefix RD 6:N and imports it into VPN 2 as RD 8:N.
6. While importing the prefix, ASBR2 sets the next hop of RD 8:N to ASBR1's interface address in VRF 2. The next hop table ID is also set to that of VRF 2. While installing the MPLS forwarding entry for RD 8:N, by default the outgoing label is not installed in forwarding. This enables traffic between the ASBRs to be IP.
7. ASBR2 advertises the imported prefix RD 8:N to PE2. It sets itself as the next hop for this prefix and also allocates a local label that is signaled with the prefix. By default, ASBR2 does not advertise the source prefix RD 6:N to PE2. This advertisement is suppressed because the prefix is being imported into an Option AB VRF.
8. PE2 imports the RD 8:N into VRF 2 as RD 4:N.

## MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding for CSC

The following sections describe MPLS VPN—Inter-AS Option AB operation for a CSC scenario for VPN 1. These sections are similar to those found in [“MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding in Non-CSC Networks”](#) section on page 4 for VPN 1, except for the method in which MPLS labels are handled between the two ASBRs.

- [Route Distribution for VPN 1, page 5](#)
- [Packet Forwarding for VPN 1, page 5](#)

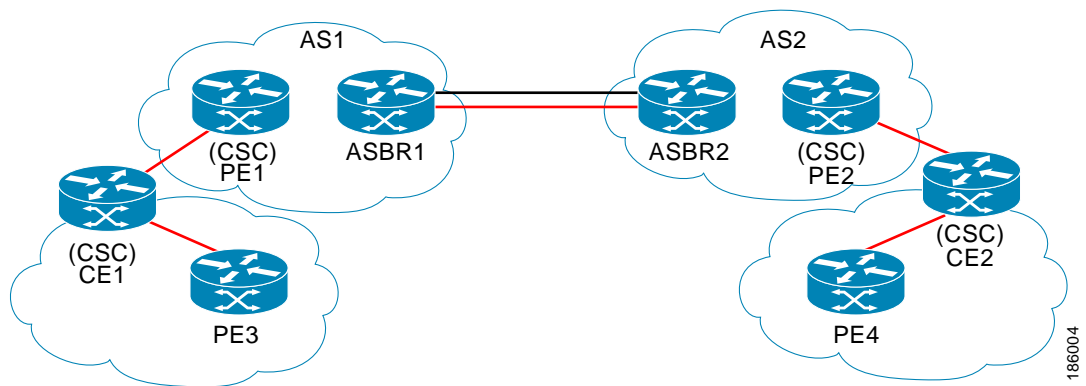


**Note**

VPN 2 is not shown or discussed in this section.

[Figure 2](#) shows how VPN 1 provides VPN service to a small customer carrier that in turn provides a VPN service to its customer. This configuration implies that VPN 1 is used to provide a Label Switched Path (LSP) between the PE (PE 3 and PE 4) loopback interfaces of the small customer carrier.

**Figure 2** *MPLS VPN Inter-AS Option AB CSC Topology*



**Note**

The RD, RT, VRF, and Link provisioning in this section is the same as in the [“MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding in Non-CSC Networks”](#) section on page 4 example for VPN 1.

### Route Distribution for VPN 1

The following information describe the route distribution process for VPN 1 in [Figure 1](#). Prefix “N” is used in these steps to indicate the IP address of a VPN.

1. CE1 advertises PE 3 loopback N to PE1.
2. PE1 advertises a VPN prefix RD 1:N to ASBR1 through MP-iBGP.
3. ASBR1 imports the prefix into VPN 1 and creates a prefix RD 5:N.
4. ASBR1 advertises the imported prefix RD 5:N to ASBR2. It sets itself as the next hop for this prefix and also allocates a local label that is signaled with the prefix.
5. ASBR1 advertises the route with the export RT configured on the VRF rather than the originally received RTs. By default, ASBR1 does not advertise the source prefix RD 1:N to ASBR2. This advertisement is suppressed as the prefix is being imported into an Option AB VRF.

**Note**

In an Option 10B connection, the source prefix can be advertised to another ASBR on which ASBR1 has an Option 10B connection. An ASBR with an Option 10B connection maintains all VPNv4 routes in its BGP table.

6. ASBR2 receives the prefix RD 5:N and imports it into VPN 1 as RD 7:N.
7. ASBR2 advertises the route with the export RT configured on the VRF rather than the originally received RTs.
8. While importing the prefix, ASBR2 sets the next hop of RD 7:N to ASBR1 interface address in VRF 1. The next hop table ID is also set to that of VRF 1.

**Note**

In a CSC scenario, an outgoing MPLS label can be installed in forwarding by making a configuration change. See [“How to Configure Inter-AS Option AB” section on page 9](#).

9. While installing the MPLS forwarding entry for RD 7:N, the outgoing label is installed during the forwarding process, which enables the traffic between the ASBRs to be MPLS traffic.
10. ASBR2 advertises the imported prefix RD 7:N to PE2. It sets itself as the next hop for this prefix and also allocates a local label that is signaled with the prefix. By default, ASBR2 does not advertise the source prefix RD 5:N to PE2. This advertisement is suppressed as the prefix is being imported into an Option AB VRF.
11. PE2 imports the RD 7:N into VRF 1 as RD 3:N.

## Packet Forwarding for VPN 1

The packet forwarding process shown below works the same as it does in an Option A scenario. See [“MPLS VPN—Inter-AS Option AB Route Distribution and Packet Forwarding in Non-CSC Networks” section on page 4](#) for more information about Option A.

1. PE 4 sends an MPLS packet destined for N to CE2.
2. CE2 swaps the MPLS label and sends a packet destined for N to PE2.
3. PE2 encapsulates the packet with the VPN label allocated by ASBR2 and the IGP label needed to tunnel the packet to ASBR2.
4. The packet arrives on ASBR2 with the VPN label. ASBR2 swaps the received VPN label with the outgoing label received from ASBR1 and sends the MPLS packet on to the VRF 1 interface.
5. The MPLS packet arrives at ASBR1 on the VRF 1 interface. ASBR1 then swaps the received MPLS label with a label stack consisting of the VPN label allocated by PE1 and the IGP label needed to tunnel the packet to PE1.
6. The packet arrives on PE1 with the VPN label. PE1 disposes the VPN label and forwards the MPLS packet to CE1. CE1 in turn swaps the label and forwards the labeled packet to PE 3.

# How to Configure Inter-AS Option AB

The following sections describe how to configure the Inter-AS Option AB feature on an ASBR for either an MPLS VPN or an MPLS VPN that supports CSC:

- [Configuring an Inter-AS Option AB Connection, page 9](#)
- [Changing an Inter-AS Option A Deployment to an Option AB Deployment, page 15](#)

## Configuring an Inter-AS Option AB Connection

The following sections are required and describe how to configure an Inter-AS Option AB connection on an ASBR:

- [Configuring the VRFs on the ASBR Interface for Each VPN Customer, page 9](#)
- [Configuring the MP-BGP Session Between ASBR Peers, page 11](#)
- [Configuring the Routing Policy for VPNs that Need Inter-AS Connections, page 13](#)

**Note**

See the [Configuring MPLS Layer 3 VPNs](#) feature module for more information on configuring PE and CE routers in an MPLS VPN.

## Configuring the VRFs on the ASBR Interface for Each VPN Customer

Use the following steps to configure the VRFs on the ASBR interface for each VPN customer so that these VPNs have connectivity over the MPLS VPN—Inter-AS Option AB network.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *vrf-name*
5. **mpls bgp forwarding** (Optional)
6. **end**

**Note**

The **mpls bgp forwarding** command is used only on the ASBR interface for VRFs that support CSC.

Use all of the steps in the following procedure to configure additional VRFs that need to be configured on the ASBR interface and the VRFs that need to be configured on the peer ASBR interface.

## DETAILED STEPS

|        | Command or Action                                                                                            | Purpose                                                                                                                                                                                                                                                                                                 |
|--------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                       | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                        |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                               | Enters global configuration mode.                                                                                                                                                                                                                                                                       |
| Step 3 | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config)# interface Ethernet 5/0         | Specifies the interface to configure and enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type</i> argument specifies the type of interface to be configured.</li> <li>The <i>number</i> argument specifies the port, connector, or interface card number.</li> </ul> |
| Step 4 | <b>ip vrf forwarding</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config-if)# ip vrf forwarding vpn1 | Associates a VRF with the specified interface or subinterface. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                            |
| Step 5 | <b>mpls bgp forwarding</b><br><br><b>Example:</b><br>Router(config-if)# mpls bgp forwarding                  | (Optional) This step applies to a CSC network only. Configures BGP to enable MPLS forwarding on connecting interfaces for VRFs that must support MPLS traffic.                                                                                                                                          |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# end                                                  | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                               |

## Configuring the MP-BGP Session Between ASBR Peers

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (see RFC 2283, *Multiprotocol Extensions for BGP-4*), which define support for address families other than IPv4. Using the extensions ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

Follow the steps in this section to configure the MP-BGP session on the ASBR.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *as-number*
5. **address-family vpnv4** [**unicast**]
6. **neighbor** {*ip-address* | *peer-group-name*} **activate**
7. **neighbor** {*ip-address* | *peer-group-name*} **inter-as-hybrid**
8. **exit-address-family**
9. **end**

Use all of the steps in the following procedure to configure the MP BGP session on the peer ASBR.

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100                                                                                                | Configures a BGP routing process and places the router in router configuration mode.<br><br>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535. |
| Step 4 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>remote-as</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config-router)# neighbor 192.168.0.1<br>remote-as 200 | Adds an entry to the BGP or multiprotocol BGP neighbor table. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>The <i>as-number</i> argument specifies the autonomous system to which the neighbor belongs.</li> </ul>                         |
| Step 5 | <b>address-family</b> <b>vpn4</b> [ <b>unicast</b> ]<br><br><b>Example:</b><br>Router(config-router)# address-family vpn4                                                                  | Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes. <ul style="list-style-type: none"> <li>The <b>unicast</b> keyword specifies IPv4 unicast address prefixes.</li> </ul>                                                                                                                                                     |
| Step 6 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>activate</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.0.1<br>activate                     | Enables the exchange of information with a neighboring router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul>                                                                                                                              |

|        | Command or Action                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 7 | <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> }<br><b>inter-as-hybrid</b><br><br><b>Example:</b><br>Router(config-router-af)# neighbor 192.168.0.1<br>inter-as-hybrid | Configures eBGP peer router (ASBR) as an Inter-AS Option AB peer. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> <li>If any prefixes are imported into Option AB VRFs, then the imported paths are advertised to this peer.</li> <li>If any prefixes are received from this peer and are imported into Option AB VRFs, then the imported paths are advertised to iBGP peers.</li> </ul> <b>Note</b> Advertised routes have RTs that are configured on the VRF. Advertised routes do not have their original RTs. |
| Step 8 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                                                                                   | Exits from the address family configuration submode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Step 9 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                                                                                   | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

## Configuring the Routing Policy for VPNs that Need Inter-AS Connections

Use the steps in this section to configure VRFs for the VPNs that need Inter-AS connections between ASBR peers, by configuring the appropriate routing policy and Option AB configuration.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **rd** *route-distinguisher*
5. **address-family** **ipv4**
6. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
7. **inter-as-hybrid** [**csc**]
8. **inter-as-hybrid** [**csc**] **next-hop** *ip-address*
9. **exit**

Use all of the steps in the following procedure to configure additional VPNs that need Inter-AS Option AB connectivity on this ASBR and the peer ASBR.



## DETAILED STEPS

|        | Command or Action                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                      | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Step 3 | <b>vrf definition</b> <i>vrf-name</i><br><br><b>Example:</b><br>Router(config)# vrf definition vpn1                                                                                 | Defines the VPN routing instance by assigning a VRF name and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Step 4 | <b>rd</b> <i>route-distinguisher</i><br><br><b>Example:</b><br>Router(config-vrf)# rd 100:1                                                                                         | Creates routing and forwarding tables. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter an RD in either of these formats: <ul style="list-style-type: none"> <li>16-bit autonomous system number: your 32-bit number, for example, 101:3</li> <li>32-bit IP address: your 16-bit number, for example, 192.168.122.15:1</li> </ul> </li> </ul>                                                                                                                                                                                                   |
| Step 5 | <b>address-family</b> <i>ipv4</i><br><br><b>Example:</b><br>Router(config-vrf)# address-family ipv4                                                                                 | Enters VRF address family configuration mode to specify an address family for a VRF. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies an IPv4 address family for a VRF.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 6 | <b>route-target</b> { <b>import</b>   <b>export</b>   <b>both</b> }<br><i>route-target-ext-community</i><br><br><b>Example:</b><br>Router(config-vrf-af)# route-target import 100:1 | Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword imports routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword exports routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword imports routing information from and exports routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF list of import, export, or both (import and export) route-target extended communities.</li> </ul> |

|               | Command or Action                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b> | <b>inter-as-hybrid</b> [ <i>csc</i> ]<br><br><b>Example:</b><br>Router(config-vrf-af)# <b>inter-as-hybrid</b>                                                        | Specifies the VRF as an Option AB VRF, which has the following effects: <ul style="list-style-type: none"> <li>• Routes imported to this VRF can be advertised to Option AB peers and VPNv4 iBGP peers.</li> <li>• When routes received from Option AB peers and are imported into the VRF, the next hop table ID of the route is set to the table ID of the VRF.</li> <li>• If the <b>csc</b> keyword is not used, a per-VRF label is allocated for imported routes.</li> <li>• When routes are received from Option AB peers and are imported next into the VRF, the learned out label can only be installed in forwarding when the <b>csc</b> keyword is used.</li> </ul> The <b>csc</b> keyword implies the following: <ul style="list-style-type: none"> <li>• A per-prefix label is allocated for imported routes.</li> <li>• For routes received from Option AB peers that are imported into the VRF, the learned out label is installed in forwarding.</li> </ul> |
| <b>Step 8</b> | <b>inter-as-hybrid</b> [ <i>csc</i> ] <b>next-hop</b> <i>ip-address</i><br><br><b>Example:</b><br>Router(config-vrf-af)# <b>inter-as-hybrid next-hop</b> 192.168.1.0 | (Optional) Specifies the next hop IP address to be set on paths that are imported into the VRF and that are received from an Option AB peer. The next hop context is also set to the VRF, which imports these paths.<br><br>The <b>csc</b> keyword implies the following: <ul style="list-style-type: none"> <li>• A per-prefix label is allocated for imported routes.</li> <li>• For routes received from Option AB peers that are imported into the VRF, the learned outlabel is installed in forwarding.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 9</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-vrf-af)# <b>exit</b>                                                                                             | Exits to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Changing an Inter-AS Option A Deployment to an Option AB Deployment

In an Option A deployment, the VRF instances are back-to-back between the ASBR routers and there is direct connectivity between PE routers of different autonomous systems. The PE routers are attached by multiple physical or logical interfaces, each of which is associated with a given VPN (through a VRF instance).

In the Option AB deployment, the different autonomous systems interconnect by using a single MP-BGP session in the global routing table to carry control plane traffic.

Use the following steps to change an MPLS VPN Inter-AS Option A deployment to an Option AB deployment.

1. Configure the MP-BGP session on the ASBR. BGP multiprotocol extensions are used to define support for address families other than IPv4 so that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other. See [“Configuring the MP-BGP Session Between ASBR Peers” section on page 11](#) for detailed configuration information.
2. Identify the VRFs that need an upgrade from Option A and configure them for Option AB by using the **inter-as-hybrid** command. See [“Configuring the Routing Policy for VPNs that Need Inter-AS Connections” section on page 13](#) for detailed configuration information.
3. Use the following steps in this section to remove the configuration for the eBGP (peer ASBR) neighbor.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *as-number*
4. **address-family ipv4 vrf** *vrf-name*
5. **no neighbor** {*ip-address* | *peer-group-name*}
6. **exit-address-family**
7. **end**

Repeat all the steps in the following procedure to remove the configuration for additional eBGP (peer ASBR) neighbors.

## DETAILED STEPS

|        | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                       |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 3 | <b>router bgp</b> <i>as-number</i><br><br><b>Example:</b><br>Router(config)# router bgp 100 | Configures a BGP routing process and places the router in router configuration mode.<br><ul style="list-style-type: none"><li>• The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along. Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.</li></ul> |

|        | Command or Action                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                            |
|--------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 4 | <b>address-family ipv4 vrf vrf-name</b><br><br><b>Example:</b><br>Router(config-router)# address-family ipv4 vrf vpn4         | Configures each VRF that is identified in the MP-BGP session on the ASBR so that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other. Enters address family configuration mode to specify an address family for a VRF.            |
| Step 5 | <b>no neighbor {ip-address   peer-group-name}</b><br><br><b>Example:</b><br>Router(config-router-af)# no neighbor 192.168.0.1 | Removes the configuration for the exchange of information with the neighboring eBGP (ASBR) router. <ul style="list-style-type: none"> <li>The <i>ip-address</i> argument specifies the IP address of the neighbor.</li> <li>The <i>peer-group-name</i> argument specifies the name of a BGP peer group.</li> </ul> |
| Step 6 | <b>exit-address-family</b><br><br><b>Example:</b><br>Router(config-router-af)# exit-address-family                            | Exits from address family configuration mode.                                                                                                                                                                                                                                                                      |
| Step 7 | <b>end</b><br><br><b>Example:</b><br>Router(config-router-af)# end                                                            | (Optional) Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                          |

# Configuration Examples for MPLS VPN—Inter-AS Option AB

The following sections describe standard and CSC MPLS VPN configurations between two ASBR peers that use the Inter-AS AB feature:

- [Inter-AS AB Network Configuration: Examples, page 18](#)
- [Inter-AS AB CSC Configuration: Examples, page 27](#)

## Inter-AS AB Network Configuration: Examples

The following examples show the configuration of an inter-AS option AB network that uses non overlapping IP addresses:

- [CE1: Example, page 18](#)
- [CE2: Example, page 19](#)
- [PE1: Example, page 19](#)
- [Route Reflector 1: Example, page 20](#)
- [ASBR1: Example, page 21](#)
- [ASBR 3: Example, page 23](#)
- [PE2: Example, page 24](#)
- [CE3: Example, page 26](#)
- [CE 4: Example, page 26](#)

### CE1: Example

```
!
ip cef distributed
!
interface lo0
 ip address 192.168.13.13 255.255.255.255
 no shutdown
!
interface et4/0
 ip address 192.168.36.1 255.255.255.0
 no shutdown
!
router ospf 300
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface et4/0
 network 192.168.13.13 0.0.0.0 area 300
!
router bgp 300
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.36.2 remote-as 100
 neighbor 192.168.36.2 advertisement-interval 5
 address-family ipv4 no auto-summary
 redistribute connected
 neighbor 192.168.36.2 activate
```

## CE2: Example

```

!
ip cef distributed
!
interface lo0
 ip address 192.168.14.14 255.255.255.255
 no shutdown
!
interface et1/6
 ip address 192.168.37.1 255.255.255.0
 no ipv6 address
 no shutdown
!
router ospf 400
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 passive-interface et1/6
 network 192.168.14.14 0.0.0.0 area 400
!
router bgp 400
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no synchronization
 neighbor 192.168.0.2 remote-as 100
 neighbor 192.168.0.2 advertisement-interval 5
 address-family ipv4 no auto-summary
 redistribute connected
 neighbor 192.168.0.2 activate
!

```

## PE1: Example

```

!
ip cef distributed
!
ip vrf vpn1
 rd 100:1
  route-target import 100:1
  route-target import 200:1
  route-target export 100:1
!
ip vrf vpn2
 rd 100:2
  route-target import 100:2
  route-target import 200:2
  route-target export 100:2
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
 ip address 192.168.17.17 255.255.255.255
 no shutdown
!
interface gi3/1

```

```

ip vrf forwarding vpn1
ip address 192.168.36.2 255.255.255.0
no shutdown
!
interface gi3/8
mpls ip
mpls label protocol ldp
ip address 192.168.31.2 255.255.255.0
!
interface gi3/10
mpls ip
mpls label protocol ldp
ip address 192.168.40.1 255.255.255.0
no shutdown
!
interface gi3/13
ip vrf forwarding vpn2
ip address 192.168.0.2 255.0.0.0
no shutdown
!
router ospf 100
nsf enforce global
redistribute connected subnets
auto-cost reference-bandwidth 1000
passive-interface gi3/1
passive-interface gi3/13
network 192.168.0.0 0.0.255.255 area 10
network 192.168.17.17 0.0.0.0 area 100
network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no bgp default ipv4-unicast
no synchronization
neighbor 192.168.19.19 remote-as 100
neighbor 192.168.19.19 update-source Loopback0
address-family ipv4 vrf vpn1
no auto-summary
redistribute connected
neighbor 192.168.36.1 remote-as 300
neighbor 192.168.36.1 activate
neighbor 192.168.36.1 advertisement-interval 5
address-family ipv4 vrf vpn2 no auto-summary
redistribute connected
neighbor 192.168.37.1 remote-as 400
neighbor 192.168.37.1 activate
neighbor 192.168.37.1 advertisement-interval 5
address-family vpnv4
bgp scan-time import 5
neighbor 192.168.19.19 activate
neighbor 192.168.19.19 send-community extended
!

```

## Route Reflector 1: Example

```

!
ip cef distributed

mpls ldp router-id lo0 force
mpls ldp graceful-restart

```

```

mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls ip
mpls label protocol ldp
!
interface lo0
 ip address 192.168.19.19 255.255.255.255
 no shutdown
!
interface gi3/3
 mpls ip
 mpls label protocol ldp
 ip address 192.168.40.2 255.255.255.0
 no shutdown
!
router ospf 100
 nsf enforce global
 redistribute connected subnets
 auto-cost reference-bandwidth 1000
 network 192.168.19.19 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100 !
router bgp 100
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.11.11 remote-as 100
 neighbor 192.168.11.11 update-source Loopback0
 neighbor 192.168.17.17 remote-as 100
 neighbor 192.168.17.17 update-source Loopback0
 neighbor 192.168.11.11 route-reflector-client
 address-family ipv4
 no neighbor 192.168.17.17 activate
 neighbor 192.168.11.11 route-reflector-client
 address-family vpnv4
 bgp scan-time import 5
 neighbor 192.168.11.11 activate
 neighbor 192.168.11.11 send-community extended
 neighbor 192.168.17.17 activate
 neighbor 192.168.17.17 send-community extended
 neighbor 192.168.11.11 route-reflector-client
 neighbor 192.168.17.17 route-reflector-client
!

```

## ASBR1: Example

```

!
ip cef distributed
!
ip vrf vpn1
 rd 100:1
  route-target import 100:1
  route-target import 200:1
  route-target export 100:1
  inter-as-hybrid next-hop 192.168.32.2
exit

ip vrf vpn2
 rd 100:2
  route-target import 100:2
  route-target import 200:2
  route-target export 100:2

```



```

    inter-as-hybrid next-hop 192.168.33.2
exit
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
    mpls ip
    mpls label protocol ldp

interface lo0
    ip address 192.168.11.11 255.255.255.255
    no ipv6 address
    ip route-cache distributed
    ip route-cache cef distributed
    no shutdown

interface gi3/8
mpls ip
    mpls label protocol ldp
    ip address 192.168.13.1 255.255.255.0
    no ipv6 address
    ip route-cache distributed
    ip route-cache cef distributed
    no shutdown

interface gi3/10
    ip vrf forwarding vpn1
    ip address 192.168.32.1 255.255.255.0
    no ipv6 address
    ip route-cache distributed
    ip route-cache cef distributed
    no shutdown

interface gi3/11
    ip vrf forwarding vpn2
    ip address 192.168.33.1 255.255.255.0
    no ipv6 address
    ip route-cache distributed
    ip route-cache cef distributed
    no shutdown

interface gi3/46
    ip address 192.168.34.1 255.255.255.0
    no ipv6 address
    ip route-cache distributed
    ip route-cache cef distributed
    no shutdown

router ospf 100
    nsf enforce global
    redistribute connected subnets
    auto-cost reference-bandwidth 1000
    passive-interface gi3/10
    passive-interface gi3/11
    passive-interface gi3/46
    network 192.168.0.0 0.0.255.255 area 100
    network 192.168.11.11 0.0.0.0 area 100

router bgp 100
    bgp graceful-restart restart-time 120
    bgp graceful-restart stalepath-time 360
    bgp graceful-restart
    no synchronization

```

```

no bgp default route-target filter
bgp router-id 192.168.11.11
neighbor 192.168.34.2 remote-as 200
neighbor 192.168.34.2 advertisement-interval 5
neighbor 192.168.19.19 remote-as 100
neighbor 192.168.19.19 update-source Loopback0
address-family ipv4
  no auto-summary
address-family ipv4 vrf vpn1
  no auto-summary
address-family ipv4 vrf vpn2
  no auto-summary
address-family vpnv4
  bgp scan-time import 5
  neighbor 192.168.34.2 activate
  neighbor 192.168.34.2 send-community both
  neighbor 192.168.34.2 inter-as-hybrid
  neighbor 192.168.19.19 activate
  neighbor 192.168.19.19 send-community extended !
ip route vrf vpn1 192.168.12.12 255.255.255.255 gi3/10 192.168.32.2
ip route vrf vpn2 192.168.12.12 255.255.255.255 gi3/11 192.168.33.2
!

```

### ASBR 3: Example

```

!
ip cef distributed
!
ip vrf vpn1
  rd 200:1
  route-target import 100:1
  route-target import 200:1
  route-target export 200:1
  inter-as-hybrid next-hop 192.168.32.1
!
ip vrf vpn2
  rd 200:2
  route-target import 100:2
  route-target import 200:2
  route-target export 200:2
  inter-as-hybrid next-hop 192.168.33.1
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
  ip address 192.168.12.12 255.255.255.255
  no shutdown
!
interface po2/1/0
  mpls ip
  mpls label protocol ldp
  ip address 192.168.35.1 255.255.255.0
  crc 16
  clock source internal
  no shutdown
!
interface gi3/10

```

```

ip vrf forwarding vpn1
ip address 192.168.32.2 255.255.255.0
no shutdown
!
interface gi3/11
ip vrf forwarding vpn2
ip address 192.168.33.2 255.255.255.0
no shutdown
!
interface gi3/45
ip address 192.168.34.2 255.255.255.0
no shutdown
!
router ospf 200
nsf enforce global
redistribute connected subnets
auto-cost reference-bandwidth 1000
passive-interface gi3/10
passive-interface gi3/11
passive-interface gi3/45
network 192.168.0.0 0.0.255.255 area 200 network 192.168.12.12 0.0.0.0 area 200

router bgp 200
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no synchronization
no bgp default route-target filter
bgp router-id 192.168.12.12
neighbor 192.168.34.1 remote-as 100
neighbor 192.168.34.1 advertisement-interval 5
neighbor 192.168.20.20 remote-as 200
neighbor 192.168.20.20 update-source Loopback0
address-family ipv4
no auto-summary
address-family ipv4 vrf vpn1
no auto-summary
address-family ipv4 vrf vpn2
no auto-summary
address-family vpnv4
bgp scan-time import 5
neighbor 192.168.34.1 activate
neighbor 192.168.34.1 send-community both
neighbor 192.168.34.1 inter-as-hybrid
neighbor 192.168.20.20 activate
neighbor 192.168.20.20 send-community extended !
ip route vrf vpn1 192.168.11.11 255.255.255.255 gi3/10 192.168.32.1
ip route vrf vpn2 192.168.11.11 255.255.255.255 gi3/11 192.168.33.1
!

```

## PE2: Example

```

!
ip cef distributed
!
ip vrf vpn1
rd 200:1
route-target import 100:1
route-target import 200:1
route-target export 200:1
!
ip vrf vpn2

```

```

rd 200:2
route-target import 100:2
route-target import 200:2
route-target export 200:2
!
mpls ldp router-id lo0 force
mpls ldp graceful-restart
mpls ip
mpls ip propagate-ttl
mpls ldp advertise-labels
mpls label protocol ldp
!
interface lo0
ip address 192.168.18.18 255.255.255.255
no shutdown
!
interface pol/0/0
mpls ip
mpls label protocol ldp
ip address 192.168.35.2 255.255.255.0
crc 16
clock source internal
no shutdown
!
interface gi3/2
ip vrf forwarding vpn1
ip address 192.168.38.2 255.255.255.0
no shutdown
!
interface gi3/8
mpls ip
mpls label protocol ldp
ip address 192.168.4.1 255.255.255.0
no shutdown
!
interface gi3/10
ip vrf forwarding vpn2
ip address 192.168.39.2 255.255.255.0
no shutdown
!
router ospf 200
nsf enforce global
redistribute connected subnets
auto-cost reference-bandwidth 1000
passive-interface gi3/10
passive-interface gi3/2
network 192.168.0.0 0.0.255.255 area 200
network 192.168.18.18 0.0.0.0 area 200
network 192.168.0.0 0.0.255.255 area 200 !
router bgp 200
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no bgp default ipv4-unicast
no synchronization
neighbor 192.168.20.20 remote-as 200
neighbor 192.168.20.20 update-source Loopback0
address-family ipv4 vrf vpn1
no auto-summary
redistribute connected
neighbor 192.168.38.1 remote-as 500
neighbor 192.168.38.1 activate
neighbor 192.168.38.1 advertisement-interval 5
address-family ipv4 vrf vpn2

```

```

no auto-summary
redistribute connected
neighbor 192.168.9.1 remote-as 600
neighbor 192.168.9.1 activate
neighbor 192.168.9.1 advertisement-interval 5
address-family vpnv4
  bgp scan-time import 5
neighbor 192.168.20.20 activate
neighbor 192.168.20.20 send-community extended
!
```

## CE3: Example

```

!
ip cef distributed
!
interface lo0
ip address 192.168.15.15 255.255.255.255
no shutdown
!
interface gi0/2
ip address 192.168.38.1 255.255.255.0
no shutdown
!
router ospf 500
  nsf enforce global
  redistribute connected subnets
  auto-cost reference-bandwidth 1000
  passive-interface gi0/2
  network 192.168.15.15 0.0.0.0 area 500
!
router bgp 500
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no synchronization
  neighbor 192.168.38.2 remote-as 200
  neighbor 192.168.38.2 advertisement-interval 5
  address-family ipv4
  no auto-summary
  redistribute connected
  neighbor 192.168.38.2 activate
!
```

## CE 4: Example

```

!
ip cef distributed
!
interface lo0
ip address 192.168.16.16 255.255.255.255
no shutdown
!
interface et6/2
ip address 192.168.9.1 255.255.255.0
no shutdown
!
router ospf 600
  nsf enforce global
  redistribute connected subnets
  auto-cost reference-bandwidth 1000
```

```
passive-interface et6/2
network 192.168.16.16 0.0.0.0 area 600
!
router bgp 600
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  no synchronization
  neighbor 192.168.39.2 remote-as 200
  neighbor 192.168.39.2 advertisement-interval 5
  address-family ipv4 no auto-summary
  redistribute connected
  neighbor 192.168.39.2 activate
!
```

## Inter-AS AB CSC Configuration: Examples

The following examples show the configuration of an inter-AS option AB network with CSC:

- [CE1: Example, page 27](#)
- [CE2: Example, page 28](#)
- [CE3: Example, page 28](#)
- [CE 4: Example, page 29](#)
- [PE1: Example, page 29](#)
- [CSC-CE1: Example, page 30](#)
- [CSC-PE1: Example, page 31](#)
- [PE 2: Example, page 32](#)
- [CSC-CE2: Example, page 33](#)
- [ASBR1: Example, page 34](#)
- [CSC-PE 3: Example, page 37](#)
- [CSC-CE3: Example, page 39](#)
- [CSC-CE 4: Example, page 39](#)
- [PE 3: Example, page 40](#)
- [PE 4: Example, page 41](#)

### CE1: Example

```
!
ip cef distributed
!
interface Loopback0
  ip address 192.168.20.20 255.255.255.255
!
interface Ethernet3/3
  ip address 192.168.41.2 255.255.255.0
!
!
router bgp 500
  bgp router-id 192.168.20.20
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
```

```

bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 192.168.4.1 remote-as 300
!
address-family ipv4
 redistribute connected
 neighbor 192.168.4.1 activate
 neighbor 192.168.4.1 advertisement-interval 5
 no auto-summary
 no synchronization
exit-address-family
!

```

## CE2: Example

```

!
ip cef distributed
!
interface Loopback0
 ip address 192.168.21.21 255.255.255.255
!
interface Ethernet0/0/7
 ip address 192.168.42.2 255.255.255.0
!
router bgp 600
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart neighbor 192.168.42.1 remote-as 400
!
address-family ipv4
 redistribute connected
 neighbor 192.168.42.1 activate
 neighbor 192.168.42.1 advertisement-interval 5
 no auto-summary
 no synchronization
exit-address-family
!

```

## CE3: Example

```

!
ip cef distributed
!
interface Loopback0
 ip address 192.168.22.22 255.255.255.255
!
interface Ethernet6/2
 ip address 192.168.43.2 255.255.255.0
!
router bgp 500
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart neighbor 192.168.43.1 remote-as 300
!
address-family ipv4
 redistribute connected
 neighbor 192.168.43.1 activate
 neighbor 192.168.43.1 advertisement-interval 5
 no auto-summary

```

```

    no synchronization
  exit-address-family
!
```

## CE 4: Example

```

!
ip cef distributed
!
interface Loopback0
 ip address 192.168.23.23 255.255.255.255
!
!
interface Ethernet0/0/7
 ip address 192.168.44.2 255.255.255.0
!
router bgp 600
 bgp router-id 192.168.23.23
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.44.1 remote-as 400
!
 address-family ipv4
  redistribute connected
  neighbor 192.168.44.1 activate
  neighbor 192.168.44.1 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!
```

## PE1: Example

```

!
ip cef distributed
!
ip vrf vpn3
 rd 300:3
 route-target export 300:3
 route-target import 300:3
!
mpls ldp graceful-restart
!
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.192.10 255.255.255.255
!
interface Ethernet3/1
 ip vrf forwarding vpn3
 ip address 192.168.4.1 255.255.255.0
!
interface Ethernet5/3
 ip address 192.168.3.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
```



```

!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 network 192.168.192.10 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
!
router bgp 300
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.19.19 remote-as 300
 neighbor 192.168.19.19 update-source Loopback0
!
 address-family vpnv4
  neighbor 192.168.19.19 activate
  neighbor 192.168.19.19 send-community extended
  bgp scan-time import 5
 exit-address-family
!
 address-family ipv4 vrf vpn3
  redistribute connected
  neighbor 192.168.41.2 remote-as 500
  neighbor 192.168.41.2 activate
  neighbor 192.168.41.2 as-override
  neighbor 192.168.41.2 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!

```

## CSC-CE1: Example

```

!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.11.11 255.255.255.255
!
!
interface Ethernet3/4
 ip address 192.168.30.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 300 metric 3 subnets
 passive-interface FastEthernet1/0
 network 192.168.11.11 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
 distance ospf intra-area 19 inter-area 19

```

```

!
router bgp 300
  bgp router-id 192.168.11.11
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 192.168.13.1 remote-as 100
!
address-family ipv4
  redistribute ospf 300 metric 4 match internal external 1 external 2
  neighbor 192.168.13.1 activate
  neighbor 192.168.13.1 send-label
  no auto-summary
  no synchronization
exit-address-family
!

```

## CSC-PE1: Example

```

!
ip vrf vpn1
  rd 100:1
  route-target export 100:1
  route-target import 100:1
  route-target import 100:5
  route-target import 200:1
!
ip vrf vpn2
  rd 100:2
  route-target export 100:2
  route-target import 100:2
  route-target import 100:6
  route-target import 200:2
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
  ip address 192.168.12.12 255.255.255.255
!
!
interface FastEthernet4/0/0
  ip address 192.168.34.1 255.255.255.0
  mpls label protocol ldp
  mpls ip
!
interface FastEthernet4/0/1
  ip vrf forwarding vpn1
  ip address 192.168.13.1 255.255.255.0
  mpls bgp forwarding
!
!
interface FastEthernet4/1/0
  ip vrf forwarding vpn2
  ip address 192.168.33.1 255.255.255.0
  mpls bgp forwarding
!
router ospf 100

```

```

log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
network 192.168.12.12 0.0.0.0 area 100
network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
  bgp router-id 192.168.12.12
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 192.168.15.15 remote-as 100
  neighbor 192.168.15.15 update-source Loopback0
  !
  address-family vpnv4
    neighbor 192.168.15.15 activate
    neighbor 192.168.15.15 send-community extended
    bgp scan-time import 5
  exit-address-family
  !
  address-family ipv4 vrf vpn2
    neighbor 192.168.33.2 remote-as 400
    neighbor 192.168.33.2 update-source FastEthernet4/1/0
    neighbor 192.168.33.2 activate
    neighbor 192.168.33.2 as-override
    neighbor 192.168.33.2 advertisement-interval 5
    neighbor 192.168.33.2 send-label
    no auto-summary
    no synchronization
  exit-address-family
  !
  address-family ipv4 vrf vpn1
    neighbor 192.168.31.2 remote-as 300
    neighbor 192.168.31.2 update-source FastEthernet4/0/1
    neighbor 192.168.31.2 activate
    neighbor 192.168.31.2 as-override
    neighbor 192.168.31.2 advertisement-interval 5
    neighbor 192.168.31.2 send-label
    no auto-summary
    no synchronization
  exit-address-family
  !

```

## PE 2: Example

```

ip cef distributed
!
ip vrf vpn4
  rd 400:4
  route-target export 400:4
  route-target import 400:4
!
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0

```

```

ip address 192.168.13.13 255.255.255.255
!
!
interface Ethernet4/1/2
ip vrf forwarding vpn4
ip address 192.168.42.1 255.255.255.0
!
!
interface Ethernet4/1/6
ip address 192.168.32.1 255.255.255.0
mpls label protocol ldp
mpls ip
!
!
router ospf 400
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
network 192.168.13.13 0.0.0.0 area 400
network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
bgp router-id 192.168.13.13
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 192.168.25.25 remote-as 400
neighbor 192.168.25.25 update-source Loopback0
!
address-family vpnv4
neighbor 192.168.25.25 activate
neighbor 192.168.25.25 send-community extended
bgp scan-time import 5
exit-address-family
!
address-family ipv4 vrf vpn4
redistribute connected
neighbor 192.168.42.2 remote-as 600
neighbor 192.168.42.2 activate
neighbor 192.168.42.2 as-override
neighbor 192.168.42.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
!

```

## CSC-CE2: Example

```

!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
interface Loopback0
ip address 192.168.14.14 255.255.255.255
!
!

```

```

interface GigabitEthernet8/16
 ip address 192.168.33.2 255.255.255.0
 mpls bgp forwarding
!
!
interface GigabitEthernet8/24
 ip address 192.168.32.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 redistribute bgp 400 metric 3 subnets
 passive-interface GigabitEthernet8/16
 network 192.168.14.14 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
 distance ospf intra-area 19 inter-area 19
!
router bgp 400
 bgp router-id 192.168.14.14
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.33.1 remote-as 100
!
 address-family ipv4
  no synchronization
  redistribute connected
  redistribute ospf 400 metric 4 match internal external 1 external 2
  neighbor 192.168.33.1 activate
  neighbor 192.168.33.1 advertisement-interval 5
  neighbor 192.168.33.1 send-label
  no auto-summary
 exit-address-family
!

```

## ASBR1: Example

```

!
ip vrf vpn5
 rd 100:5
 route-target export 100:5
 route-target import 100:5
 route-target import 100:1
 route-target import 200:5
 inter-as-hybrid csc next-hop 192.168.35.2
!
ip vrf vpn6
 rd 100:6
 route-target export 100:6
 route-target import 100:6
 route-target import 100:2
 route-target import 200:6
 inter-as-hybrid csc next-hop 192.168.36.2
!
mpls ldp graceful-restart

```

```
mpls label protocol ldp
!
!
interface Loopback0
 ip address 192.168.15.15 255.255.255.255
!
interface GigabitEthernet2/3
 ip vrf forwarding vpn5
 ip address 192.168.35.1 255.255.255.0
 mpls bgp forwarding
!
interface GigabitEthernet2/4
 ip vrf forwarding vpn6
 ip address 192.168.36.1 255.255.255.0
 mpls bgp forwarding
!
!
interface GigabitEthernet2/5
 ip address 192.168.34.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
interface GigabitEthernet2/16
 ip address 192.168.37.1 255.255.255.0
 mpls bgp forwarding
!
!
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.15.15 0.0.0.0 area 100
 network 192.168.0.0 0.0.255.255 area 100
!
router bgp 100
 bgp router-id 192.168.15.15
 no bgp default ipv4-unicast
 no bgp default route-target filter
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.12.12 remote-as 100
 neighbor 192.168.12.12 update-source Loopback0
 neighbor 192.168.0.2 remote-as 200
 neighbor 192.168.0.2 disable-connected-check
!
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
!
 address-family vpnv4
  neighbor 192.168.12.12 activate
  neighbor 192.168.12.12 send-community extended
  neighbor 192.168.0.2 activate
  neighbor 192.168.0.2 send-community extended
  neighbor 192.168.0.2 inter-as-hybrid
 exit-address-family
!
 address-family ipv4 vrf vpn5
  no synchronization
```

```

exit-address-family
!
address-family ipv4 vrf vpn6
  no synchronization
exit-address-family
!
ip route 192.168.16.16 255.255.255.255 GigabitEthernet2/16 192.168.0.2
ip route vrf vpn5 192.168.16.16 255.255.255.255 GigabitEthernet2/3 192.168.35.2
ip route vrf vpn6 192.168.16.16 255.255.255.255 GigabitEthernet2/4 192.168.36.2
!
ip vrf vpn5
  rd 200:5
  route-target export 200:5
  route-target import 200:5
  route-target import 200:1
  route-target import 100:1
  route-target import 100:5
  inter-as-hybrid csc next-hop 192.168.35.1
!
ip vrf vpn6
  rd 200:6
  route-target export 200:6
  route-target import 200:6
  route-target import 200:2
  route-target import 100:2
  route-target import 100:6
  inter-as-hybrid csc next-hop 192.168.36.1
!
mpls ldp graceful-restart
mpls label protocol ldp
!
!
interface Loopback0
  ip address 192.168.16.16 255.255.255.255
!
!
interface GigabitEthernet3/1
  ip vrf forwarding vpn5
  ip address 192.168.35.2 255.255.255.0
  mpls bgp forwarding
!
interface GigabitEthernet3/2
  ip vrf forwarding vpn6
  ip address 192.168.36.2 255.255.255.0
  mpls bgp forwarding
!
!
interface GigabitEthernet3/14
  ip address 192.168.0.2 255.0.0.0
  mpls bgp forwarding
!
interface GigabitEthernet3/15
  ip address 192.168.38.2 255.255.255.0
  mpls label protocol ldp
  mpls ip
!
router ospf 200
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  nsf enforce global
  redistribute connected subnets
  network 192.168.16.16 0.0.0.0 area 200
  network 192.168.0.0 0.0.255.255 area 200
!
router bgp 200

```

```

bgp router-id 192.168.16.16
no bgp default ipv4-unicast
no bgp default route-target filter
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 192.168.17.17 remote-as 200
neighbor 192.168.17.17 update-source Loopback0
neighbor 192.168.37.1 remote-as 100
neighbor 192.168.37.1 disable-connected-check
!
address-family ipv4
  no synchronization
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 192.168.17.17 activate
  neighbor 192.168.17.17 send-community extended
  neighbor 192.168.37.1 activate
  neighbor 192.168.37.1 send-community extended
  neighbor 192.168.37.1 inter-as-hybrid
exit-address-family
!
address-family ipv4 vrf vpn5
  no synchronization
exit-address-family
!
address-family ipv4 vrf vpn6
  no synchronization
exit-address-family
!
ip route 192.168.15.15 255.255.255.255 GigabitEthernet3/14 192.168.37.1
ip route vrf vpn5 192.168.15.15 255.255.255.255 GigabitEthernet3/1 192.168.35.1
ip route vrf vpn6 192.168.15.15 255.255.255.255 GigabitEthernet3/2 192.168.36.1
!

```

## CSC-PE 3: Example

```

ip vrf vpn1
  rd 200:1
  route-target export 200:1
  route-target import 200:1
  route-target import 200:5
  route-target import 100:1
!
ip vrf vpn2
  rd 200:2
  route-target export 200:2
  route-target import 200:2
  route-target import 200:6
  route-target import 100:2
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
  ip address 192.168.17.17 255.255.255.255
!

```



```

interface FastEthernet4/0/2
 ip vrf forwarding vpn2
 ip address 192.168.5.1 255.255.255.0
 mpls bgp forwarding
!
!
interface FastEthernet4/0/4
 ip vrf forwarding vpn1
 ip address 192.168.9.1 255.255.255.0
 mpls bgp forwarding
!
!
interface FastEthernet4/0/7
 ip address 192.168.38.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
router ospf 200
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.17.17 0.0.0.0 area 200
 network 192.168.0.0 0.0.255.255 area 200
!
router bgp 200
 bgp router-id 192.168.17.17
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.16.16 remote-as 200
 neighbor 192.168.16.16 update-source Loopback0
!
 address-family vpnv4
  neighbor 192.168.16.16 activate
  neighbor 192.168.16.16 send-community extended
  bgp scan-time import 5
 exit-address-family
!
 address-family ipv4 vrf vpn2
  neighbor 192.168.55.0 remote-as 400
  neighbor 192.168.55.0 update-source FastEthernet4/0/2
  neighbor 192.168.55.0 activate
  neighbor 192.168.55.0 as-override
  neighbor 192.168.55.0 advertisement-interval 5
  neighbor 192.168.55.0 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
 address-family ipv4 vrf vpn1
  neighbor 192.168.39.2 remote-as 300
  neighbor 192.168.39.2 update-source FastEthernet4/0/4
  neighbor 192.168.39.2 activate
  neighbor 192.168.39.2 as-override
  neighbor 192.168.39.2 advertisement-interval 5
  neighbor 192.168.39.2 send-label
  no auto-summary
  no synchronization
 exit-address-family
!

```

## CSC-CE3: Example

```
!
interface Loopback0
 ip address 192.168.18.18 255.255.255.255
!
!
interface Ethernet3/3
 ip address 192.168.40.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!
interface FastEthernet5/0
 ip address 192.168.39.2 255.255.255.0
 mpls bgp forwarding
!
!
router ospf 300
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 300 metric 3 subnets
 network 192.168.18.18 0.0.0.0 area 300
 network 192.168.0.0 0.0.255.255 area 300
 distance ospf intra-area 19 inter-area 19
!
router bgp 300
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.9.1 remote-as 200
!
 address-family ipv4
  redistribute connected
  redistribute ospf 300 metric 4 match internal external 1 external 2
  neighbor 192.168.9.1 activate
  neighbor 192.168.9.1 advertisement-interval 5
  neighbor 192.168.9.1 send-label
  no auto-summary
  no synchronization
 exit-address-family
!
```

## CSC-CE 4: Example

```
!
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
mpls ip
!
interface Loopback0
 ip address 192.168.24.24 255.255.255.255
!
!
interface FastEthernet1/1
 ip address 192.168.55.0 255.255.255.0
 mpls bgp forwarding
```

```

!
!
interface Ethernet3/5
 ip address 192.168.56.2 255.255.255.0
 mpls label protocol ldp
 mpls ip

!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 redistribute bgp 400 metric 3 subnets
 network 192.168.24.24 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
 bgp log-neighbor-changes
 neighbor 192.168.5.1 remote-as 200
!
 address-family ipv4
  redistribute connected
  redistribute ospf 400 metric 4 match internal external 1 external 2
  neighbor 192.168.5.1 activate
  neighbor 192.168.5.1 advertisement-interval 5
  neighbor 192.168.5.1 send-label
  no auto-summary
  no synchronization
 exit-address-family

```

## PE 3: Example

```

!
ip cef distributed
!
ip vrf vpn3
 rd 300:3
 route-target export 300:3
 route-target import 300:3
 mpls ip
!
!
 mpls ldp graceful-restart
 mpls label protocol ldp
!
!
interface Loopback0
 ip address 192.168.19.19 255.255.255.255
!
!
interface Ethernet5/1/1
 ip vrf forwarding vpn3
 ip address 192.168.43.1 255.255.255.0
!
!
interface Ethernet5/1/4
 ip address 192.168.40.1 255.255.255.0
 mpls label protocol ldp
 mpls ip
!
!

```

```

router ospf 300
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  nsf enforce global
  redistribute connected subnets
  network 192.168.19.19 0.0.0.0 area 300
  network 192.168.0.0 0.0.255.255 area 300
  network 192.168.0.0 0.0.255.255 area 300
!
router bgp 300
  bgp router-id 192.168.19.19
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  neighbor 192.168.192.10 remote-as 300
  neighbor 192.168.192.10 update-source Loopback0
!
  address-family ipv4
    no neighbor 192.168.192.10 activate
    no auto-summary
    no synchronization
  exit-address-family
!
  address-family vpnv4
    neighbor 192.168.192.10 activate
    neighbor 192.168.192.10 send-community extended
    bgp scan-time import 5
  exit-address-family
!
  address-family ipv4 vrf vpn3
    neighbor 192.168.43.2 remote-as 500
    neighbor 192.168.43.2 activate
    neighbor 192.168.43.2 as-override
    neighbor 192.168.43.2 advertisement-interval 5
    no auto-summary
    no synchronization
  exit-address-family

```

## PE 4: Example

```

!
ip cef distributed
!
ip vrf vpn4
  rd 400:4
  route-target export 400:4
  route-target import 400:4
!
mpls ldp graceful-restart
mpls ldp protocol ldp
!
mpls ip
!
interface Loopback0
  ip address 192.168.25.25 255.255.255.255
!
!
interface Ethernet5/0/4
  ip address 192.168.56.1 255.255.255.0
  mpls label protocol ldp
  mpls ip

```

```

!
!
interface Ethernet5/0/7
 ip vrf forwarding vpn4
 ip address 192.168.44.1 255.255.255.0
!
!
router ospf 400
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 nsf enforce global
 redistribute connected subnets
 network 192.168.25.25 0.0.0.0 area 400
 network 192.168.0.0 0.0.255.255 area 400
!
router bgp 400
 bgp router-id 192.168.25.25
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 192.168.13.13 remote-as 400
 neighbor 192.168.13.13 ebgp-multihop 7
 neighbor 192.168.13.13 update-source Loopback0
!
 address-family ipv4
  no neighbor 192.168.13.13 activate
  no auto-summary
  no synchronization
 exit-address-family
!
 address-family vpnv4
  neighbor 192.168.13.13 activate
  neighbor 192.168.13.13 send-community extended
  bgp scan-time import 5
 exit-address-family
!
 address-family ipv4 vrf vpn4
  neighbor 192.168.44.2 remote-as 600
  neighbor 192.168.44.2 activate
  neighbor 192.168.44.2 as-override
  neighbor 192.168.44.2 advertisement-interval 5
  no auto-summary
  no synchronization
 exit-address-family
!

```

## Additional References

The following sections provide references related to the MPLS VPN—Inter-AS Option AB feature.

- [Related Documents, page 43](#)
- [Standards, page 43](#)
- [MIBs, page 43](#)
- [RFCs, page 43](#)
- [Technical Assistance, page 44](#)

## Related Documents

| Related Topic                    | Document Title                                                                                                                                                                                          |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPNs                        | <i>Configuring MPLS Layer 3 VPNs</i>                                                                                                                                                                    |
| MPLS VPN Interautonomous Systems | <ul style="list-style-type: none"> <li><i>MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses</i></li> <li><i>MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels</i></li> </ul> |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC      | Title                                       |
|----------|---------------------------------------------|
| RFC 2283 | <i>Multiprotocol Extensions for BGP-4</i>   |
| RFC 4366 | <i>BGP/MPLS IP Virtual Private Networks</i> |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p> |

# Feature Information for MPLS VPN—Inter-AS Option AB

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for MPLS VPN—Inter-AS Option AB

| Feature Name                | Release     | Feature Information                                                                                                                                                                                                                                                          |
|-----------------------------|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS VPN—Inter-AS Option AB | 12.2(33)SRC | This feature combines the best functionality of an inter-AS option (10) A and inter-AS option (10) B network to allow an MPLS VPN service provider to interconnect different autonomous systems to provide VPN services.<br><br>In 12.2(33)SRC, this feature was introduced. |
|                             | 15.0(1)M    | This feature was introduced in 15.0(1)M. The following commands were introduced or modified: <ul style="list-style-type: none"><li>• <b>neighbor inter-as-hybrid</b></li><li>• <b>inter-as-hybrid</b></li></ul>                                                              |



# Glossary

**autonomous system**—A collection of networks under a common administration sharing a common routing strategy.

**BGP**—Border Gateway Protocol. An interdomain routing protocol that exchanges network reachability information with other BGP systems (which may be within the same autonomous system or between multiple autonomous systems).

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers do not recognize associated MPLS VPNs.

**CSC**—Carrier Supporting Carrier. A hierarchical VPN model that allows small Service Providers, or customer carriers, to interconnect their IP or MPLS networks over an MPLS backbone. This eliminates the need for customer carriers to build and maintain their own MPLS backbone.

**eBGP**—external Border Gateway Protocol. A BGP between routers located within different autonomous systems. When two routers, located in different autonomous systems, are more than one hop away from one another, the eBGP session between the two routers is considered a multihop BGP.

**iBGP**—internal Border Gateway Protocol. A BGP between routers within the same autonomous system.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within a single autonomous system. Examples of common Internet IGP protocols include IGRP, OSPF, IS-IS, and RIP.

**IP**—Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.

**LFIB**—Label Forwarding Information Base. Data structure used in MPLS to hold information about incoming and outgoing labels and associated Forwarding Equivalence Class (FEC) packets.

**MP-BGP**—Multiprotocol BGP.

**MPLS**—Multiprotocol Label Switching. The name of the IETF working group responsible for label switching, and the name of the label switching approach it has standardized.

**NLRI**—Network Layer Reachability Information. The BGP sends routing update messages containing NLRI to describe a route and how to get there. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes; the route attributes include a BGP next hop gateway address and extended community values.

**NSF**—Nonstop forwarding enables routers to continuously forward IP packets following a Route Processor takeover or switchover to another Route Processor. NSF maintains and updates Layer 3 routing and forwarding information in the backup Route Processor to ensure that IP packets and routing protocol information are forwarded continuously during the switchover and route convergence process.

**PE router**—provider edge router. A router that is part of a service provider's network. It is connected to a customer edge (CE) router. All MPLS VPN processing occurs in the PE router.

**QoS**—quality of service. Measure of performance for a transmission system that indicates its transmission quality and service availability.

**RD**—route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN-IPv4 prefix.

**RT**—route target. Extended community attribute used to identify the VRF routing table into which a prefix is imported.

**SLA**—Service Level Agreement given to VPN subscribers.

**VPN**—Virtual Private Network. A secure MPLS-based network that shares resources on one or more physical networks (typically implemented by one or more service providers). A VPN contains geographically dispersed sites that can communicate securely over a shared backbone network.

**VRF**—VPN routing and forwarding instance. Routing information that defines a VPN site that is attached to a PE router. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 20079 Cisco Systems, Inc. All rights reserved.





## **MPLS Embedded Management and MIBs**





## MPLS EM—MPLS LSP Multipath Tree Trace

---

**First Published: December 4, 2006**

**Last Updated: February 27, 2009**

The MPLS EM—MPLS LSP Multipath Tree Trace feature provides the means to discover all possible equal-cost multipath (ECMP) routing paths of a label switched path (LSP) between an egress and ingress router. Once discovered, these paths can be retested on a periodic basis using Multiprotocol Label Switching (MPLS) LSP ping or traceroute. This feature is an extension to the MPLS LSP traceroute functionality for the tracing of IPv4 LSPs.

You can use the MPLS EM—MPLS LSP Multipath Tree Trace feature to discover all paths for an IPv4 LSP.

This implementation of the MPLS EM—MPLS LSP Multipath Tree Trace feature is based on RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

For information on the use of MPLS LSP ping and traceroute, see the [MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV](#) feature module.

Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks according to the fault, configuration, accounting, performance, and security (FCAPS) model.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS EM—MPLS LSP Multipath Tree Trace”](#) section on [page 33](#).

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for MPLS EM—MPLS LSP Multipath Tree Trace, page 2](#)
- [Restrictions for MPLS EM—MPLS LSP Multipath Tree Trace, page 2](#)
- [Information About MPLS EM—MPLS LSP Multipath Tree Trace, page 3](#)
- [How to Configure MPLS EM—MPLS LSP Multipath Tree Trace, page 4](#)
- [Configuration Examples for MPLS EM—MPLS LSP Multipath Tree Trace, page 22](#)
- [Additional References, page 31](#)
- [Command Reference, page 32](#)
- [Feature Information for MPLS EM—MPLS LSP Multipath Tree Trace, page 33](#)
- [Glossary, page 35](#)

## Prerequisites for MPLS EM—MPLS LSP Multipath Tree Trace

The following are prerequisites for using the MPLS EM—MPLS LSP Multipath Tree Trace feature:

- You must understand the concepts and know how to use MPLS LSP ping or traceroute as described in the *MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV* document.
- The routers in your network must be using an implementation based on RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.
- You should know the following about your MPLS network:
  - The topology
  - The number of links in your network
  - The expected number of LSPs, and how many LSPs
- Understand label switching, forwarding, and load balancing.

## Restrictions for MPLS EM—MPLS LSP Multipath Tree Trace

- All restrictions that apply to the MPLS LSP Ping and LSP Traceroute features also apply to the MPLS EM—MPLS LSP Multipath Tree Trace feature:
  - You cannot use the MPLS LSP Multipath Tree Trace feature to trace the path taken by AToM packets. The MPLS LSP Multipath Tree Trace feature is not supported for AToM. (MPLS LSP Ping is supported for AToM.) However, you can use the MPLS LSP Multipath Tree Trace feature to troubleshoot the Interior Gateway Protocol (IGP) LSP that is used by AToM.
  - You cannot use the MPLS LSP Multipath Tree Trace feature to validate or trace MPLS Virtual Private Networks (VPNs). Multiple LSP paths are not discovered unless all routers in the MPLS core support an RFC 4379 implementation of *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.
- MPLS LSP multipath tree trace is not expected to operate in networks that support time-to-live (TTL) hiding.

# Information About MPLS EM—MPLS LSP Multipath Tree Trace

Before using the MPLS EM—MPLS LSP Multipath Tree Trace feature, you need an understanding of the following concepts:

- [Overview of MPLS LSP Multipath Tree Trace, page 3](#)
- [Discovery of IPv4 Load Balancing Paths by MPLS LSP Multipath Tree Trace, page 3](#)
- [Echo Reply Return Codes Sent by the Router Processing Multipath LSP Tree Trace, page 4](#)

## Overview of MPLS LSP Multipath Tree Trace

As the number of MPLS deployments increases, the number of traffic types the MPLS networks carry could increase. In addition, load balancing on label switch routers (LSRs) in the MPLS network provides alternate paths for carrying MPLS traffic to a target router. The ability of service providers to monitor LSPs and quickly isolate MPLS forwarding problems is critical to their ability to offer services.

Prior to the release of the MPLS EM—MPLS LSP Multipath Tree Trace feature no automated way existed to discover all paths between provider edge (PE) routers. Troubleshooting forwarding problems between PEs was cumbersome.

The release of the MPLS EM—MPLS LSP Multipath Tree Trace feature provides an automated way to discover all paths from the ingress PE router to the egress PE router in multivendor networks that use IPv4 load balancing at the transit routers. Once the PE-to-PE paths are discovered, use MPLS LSP ping and MPLS LSP traceroute to periodically test them.

The MPLS EM—MPLS LSP Multipath Tree Trace feature requires the Cisco RFC-compliant implementation that is based on RFC 4379. If you do not have a Cisco IOS release that supports RFC 379, MPLS LSP multipath tree trace does not operate to discover all PE-to-PE paths.

## Discovery of IPv4 Load Balancing Paths by MPLS LSP Multipath Tree Trace

IPv4 load balancing at a transit router is based on the incoming label stack and the source and destination addresses in the IP header. The outgoing label stack and IP header source address remain constant for each branch being traced.

When you execute MPLS LSP multipath tree trace on the source LSR, the router needs to find the set of IP header destination addresses to use all possible output paths. The source LSR starts path discovery by sending a transit router a bitmap in an MPLS echo request. The transit router returns information in an MPLS echo request that contains subsets of the bitmap in a downstream map (DS Map) in an echo reply. The source router can then use the information in the echo reply to interrogate the next router. The source router interrogates each successive router until it finds one bitmap setting that is common to all routers along the path. The router uses TTL expiry to interrogate the routers to find the common bits.

For example, you could start path discovery by entering the following command at the source router:

```
Router# trace mpls multipath ipv4 10.131.101.129/32 hashkey ipv4 bitmap 16
```

This command sets the IP address of the target router as 10.131.101.192 255.255.255.255 and configures:

- The default hash key type to 8, which requests that an IPv4 address prefix and bit mask address set be returned in the DS Map in the echo reply.



- The bitmap size to 16. This means that MPLS LSP multipath tree trace uses 16 addresses (starting with 127.0.0.1) in the discovery of all paths of an LSP between the source router and the target router.

If you enter the **trace mpls multipath ipv4 10.131.101.129/32** command, MPLS LSP multipath tree trace uses the default hash type of 8 or IPv4 and a default bitmap size of 32. Your choice of a bitmap size depends on the number of routes in your network. If you have a large number of routes, you might need to use a larger bitmap size.

## Echo Reply Return Codes Sent by the Router Processing Multipath LSP Tree Trace

[Table 1](#) describes the characters that the router processing a multipath LSP tree trace packet returns to the sender about the failure or success of the request.

**Table 1** *Echo Reply Return Codes*

| Output Code | Echo Return Code | Meaning                                                  |
|-------------|------------------|----------------------------------------------------------|
| Period “.”  | —                | A timeout occurred before the target router could reply. |
| x           | 0                | No return code.                                          |
| M           | 1                | Malformed request.                                       |
| m           | 2                | Unsupported type, length, values (TLVs).                 |
| !           | 3                | Success.                                                 |
| F           | 4                | No Forwarding Equivalence Class (FEC) mapping.           |
| D           | 5                | DS Map mismatch.                                         |
| R           | 6                | Downstream router but not target.                        |
| U           | 7                | Reserved.                                                |
| L           | 8                | Labeled output interface.                                |
| B           | 9                | Unlabeled output interface.                              |
| f           | 10               | FEC mismatch.                                            |
| N           | 11               | No label entry.                                          |
| P           | 12               | No receive interface label protocol.                     |
| p           | 13               | Premature termination of the LSP.                        |
| X           | unknown          | Undefined return code.                                   |

## How to Configure MPLS EM—MPLS LSP Multipath Tree Trace

This section contains the following tasks:

- [Customizing the Default Behavior of MPLS Echo Packets, page 5](#) (optional)
- [Configuring MPLS LSP Multipath Tree Trace, page 7](#) (required)
- [Discovering IPv4 Load Balancing Paths Using MPLS LSP Multipath Tree Trace, page 9](#) (required)

- [Monitoring LSP Paths Discovered by MPLS LSP Multipath Tree Trace Using MPLS LSP Traceroute, page 10 \(optional\)](#)
- [Using DSCP to Request a Specific Class of Service in an Echo Reply, page 13 \(optional\)](#)
- [Controlling How a Responding Router Replies to an MPLS Echo Request, page 14 \(optional\)](#)
- [Specifying the Output Interface for Echo Packets Leaving a Router for MPLS LSP Multipath Tree Trace, page 16 \(optional\)](#)
- [Setting the Pace of MPLS Echo Request Packet Transmission for MPLS LSP Multipath Tree Trace, page 17 \(optional\)](#)
- [Enabling MPLS LSP Multipath Tree Trace to Detect LSP Breakages Caused by an Interface That Lacks an MPLS Configuration, page 18 \(optional\)](#)
- [Requesting That a Transit Router Validate the Target FEC Stack for MPLS LSP Multipath Tree Trace, page 19 \(optional\)](#)
- [Setting the Number of Timeout Attempts for MPLS LSP Multipath Tree Trace, page 21 \(optional\)](#)

## Customizing the Default Behavior of MPLS Echo Packets

Perform the following task to customize the default behavior of MPLS echo packets. You might need to customize the default echo packet encoding and decoding behavior to allow later implementations of the *Detecting MPLS Data Plane Failures* (RFC 4379) to be deployed in networks running earlier versions of the draft.

### MPLS Embedded Management Configuration

Before using the **ping mpls**, **trace mpls**, or **trace mpls multipath** command, you should consider ensuring that the router is configured to encode and decode MPLS echo packets in a format that all receiving routers in the network can understand.

LSP ping drafts after Version 3 (draft-ietf-mpls-ping-03) have undergone numerous TLV format changes, but the implementations based on different drafts might not interoperate properly.

To allow later Cisco implementations to interoperate with draft Version 3 Cisco and non-Cisco implementations, a global configuration mode (MPLS OAM configuration) allows you to encode and decode echo packets in formats specified by draft Version 3 implementations.

Unless configured otherwise, a Cisco implementation encodes and decodes echo requests assuming the version on which the Internet Engineering Task Force (IETF) implementation is based.

To allow for seamless interoperability with earlier Revision 1 and 3 images, you can use MPLS Operation, Administration, and Maintenance (OAM) configuration mode parameters to force the default behavior of the Revision 4 images to be compliant or compatible in networks with Revision 1 or Revision 3 images.

To prevent failures reported by the replying router due to TLV version issues, you should configure all routers in the core. Encode and decode MPLS echo packets in the same draft version. For example, if the network is running RFC 4379 (Cisco Revision 4) implementations but one router is capable of only Version 3 (Cisco Revision 3), configure all routers in the network to operate in Revision 3 mode.

Cisco Revision 4 is the default version. The default version is the latest LSP Ping version supported by the image on the router.

## Prerequisites

MPLS LSP Multipath Tree Trace requires RFC 4379 (Revision 4).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls oam**
4. **echo revision {3 | 4}**
5. **[no] echo vendor-extension**
6. **end**

## DETAILED STEPS

|               | Command or Action                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal              | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 3</b> | <b>mpls oam</b><br><br><b>Example:</b><br>Router(config)# mpls oam                          | Enters MPLS OAM configuration mode and customizes the default behavior of echo packets.                                                                                                                                                                                                                                                                                                                                |
| <b>Step 4</b> | <b>echo revision {3   4}</b><br><br><b>Example:</b><br>Router(config-mpls)# echo revision 4 | Customizes the default behavior of echo packets.<br><ul style="list-style-type: none"><li>• The <b>revision</b> keyword set echo packet attributes to one of the following:<ul style="list-style-type: none"><li>– <b>3</b> = draft-ietf-mpls-ping-03 (Revision 2)</li><li>– <b>4</b> = RFC 4379 compliant (default)</li></ul></li></ul><br><b>Note</b> The MPLS LSP Multipath Tree Trace feature requires Revision 4. |

|        | Command or Action                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <pre>[no] echo vendor-extension</pre> <p><b>Example:</b><br/> <pre>Router(config-mpls)# echo vendor-extension</pre></p> | <p>Customizes the default behavior of echo packets.</p> <ul style="list-style-type: none"> <li>The <b>vendor-extension</b> keyword sends the Cisco-specific extension of TLVs with the echo packets.</li> <li>The <b>no</b> form of the command allows you to disable a Cisco vendor's extension TLVs that another vendor's noncompliant implementations may not support.</li> </ul> <p>The router default is <b>echo vendor-extension</b>.</p> |
| Step 6 | <pre>end</pre> <p><b>Example:</b><br/> <pre>Router(config-mpls)# end</pre></p>                                          | <p>Exits to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                           |

## Configuring MPLS LSP Multipath Tree Trace

Perform the following task to configure MPLS multipath LSP traceroute. This task helps discover all LSPs from an egress router to an ingress router.

### Prerequisites

Cisco LSP ping or traceroute implementations based on draft-ietf-mpls-lsp-ping-11 are capable in some cases of detecting the formatting of the sender of an MPLS echo request. However, certain cases exist in which an echo request or echo reply might not contain the Cisco extension TLV. To avoid complications due to certain cases where the echo packets are decoded assuming the wrong TLV formats, configure all routers in the network to operate in the same mode.

For an MPLS LSP multipath tree trace to be successful, the implementation in your routers must support RFC 4379 on all core routers.

If all routers in the network support RFC-4379 and another vendor's implementation exists that is not capable of properly handling Cisco's vendor TLV, the routers supporting the RFC-compliant or later configuration must include commands to disable the Cisco vendor TLV extensions.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls oam**
4. **echo revision 4**
5. **[no] echo vendor-extension**
6. **end**
7. **trace mpls multipath ipv4** *destination-ip-address/destination-mask-length*
8. **debug mpls lspv multipath**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                             | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 3 | <b>mpls oam</b><br><br><b>Example:</b><br>Router(config)# mpls oam                                                                                                         | Enters MPLS OAM configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Step 4 | <b>echo revision 4</b><br><br><b>Example:</b><br>Router(config-mpls)# echo revision 4                                                                                      | Customizes the default behavior of echo packets. <ul style="list-style-type: none"> <li>The <b>revision 4</b> keywords set echo packet attributes to the default Revision 4 (RFC 4379 compliant).</li> </ul> <b>Note</b> The MPLS LSP Multipath Tree Trace feature requires Revision 4.                                                                                                                                                                                     |
| Step 5 | <b>[no] echo vendor-extension</b><br><br><b>Example:</b><br>Router(config-mpls) echo vendor-extension                                                                      | (Optional) Customizes the default behavior of echo packets. <ul style="list-style-type: none"> <li>The <b>vendor-extension</b> keyword sends the Cisco-specific extension of TLVs with the echo packets.</li> <li>The <b>no</b> form of the command allows you to disable a Cisco vendor's extension TLVs that another vendor's noncompliant implementations may not support.</li> </ul> The router default is <b>echo vendor-extension</b> .                               |
| Step 6 | <b>end</b><br><br><b>Example:</b><br>Router(config-mpls)# end                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Step 7 | <b>trace mpls multipath ipv4</b><br><i>destination-ip-address/destination-mask-length</i><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4<br>10.131.161.251/32 | Discovers all LSPs from an egress router to an ingress router. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>The <i>destination-ip-address</i> argument is the address prefix of the target to be tested.</li> <li>The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> </ul> |
| Step 8 | <b>debug mpls lspv multipath</b><br><br><b>Example:</b><br>Router# debug mpls lspv multipath                                                                               | Displays multipath information related to the MPLS LSP Multipath Tree Trace feature.                                                                                                                                                                                                                                                                                                                                                                                        |

## Discovering IPv4 Load Balancing Paths Using MPLS LSP Multipath Tree Trace

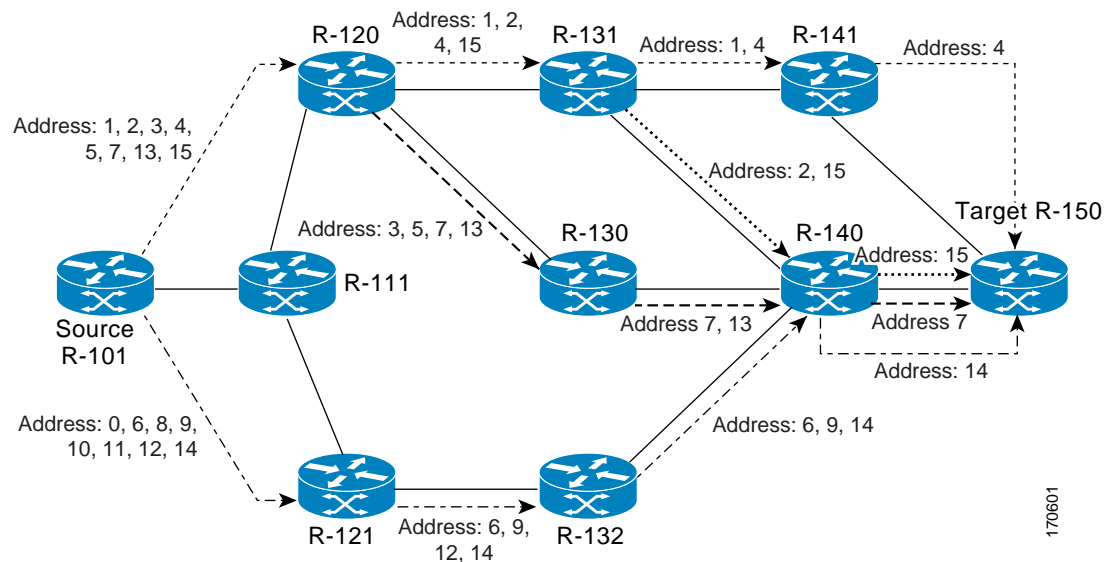
Perform the following task to discover IPv4 load balancing paths using MPLS LSP multipath tree trace.

### MPLS Multipath LSP Traceroute Path Discovery

A Cisco router load balances MPLS packets based on the incoming label stack and the source and destination addresses in the IP header. The outgoing label stack and IP header source address remain constant for each path being traced. The router needs to find the set of IP header destination addresses to use all possible output paths. This might require exhaustive searching of the 127.x.y.z/8 address space. Once you discover all paths from the source LSR to the target or destination LSR with MPLS LSP multipath tree trace, you can use MPLS LSP traceroute to monitor these paths.

Figure 1 shows how MPLS LSP multipath tree trace discovers LSP paths in a sample network. In Figure 1, the bitmap size is 16 and the numbers 0 to 15 represent the bitmapped addresses that MPLS LSP multipath tree trace uses to discover all the paths from the source LSR R-101 to the target LSR R-150. Figure 1 illustrates how the **trace mpls multipath** command discovers all LSP paths in the sample network.

**Figure 1** MPLS LSP Multipath Tree Trace Path Discovery in a Sample Network



### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls oam**
4. **echo revision 4**
5. **end**
6. **trace mpls multipath ipv4 destination-ip-address/destination-mask-length hashkey ipv4 bitmap bitmap-size**

## DETAILED STEPS

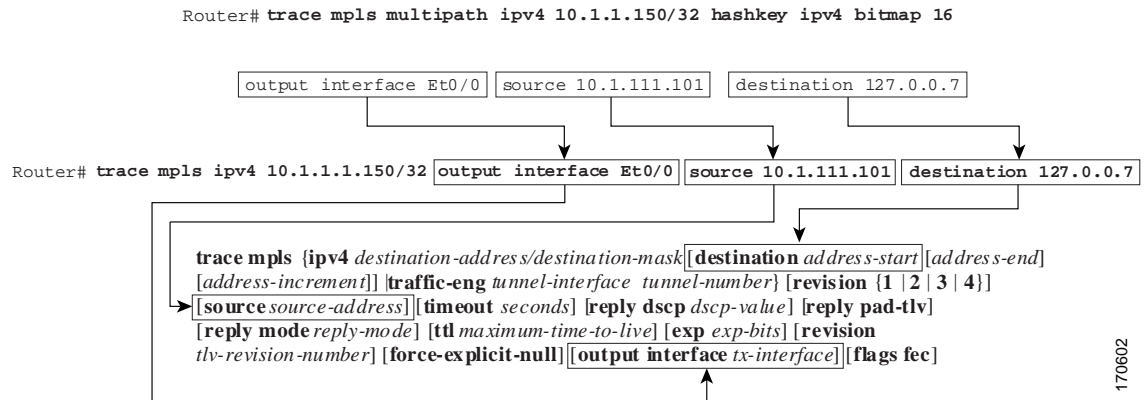
|        | Command or Action                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 3 | <b>mpls oam</b><br><br><b>Example:</b><br>Router(config)# mpls oam                                                                                                                                                | Enters MPLS OAM configuration mode and sets the echo packet attribute to Revision 4 (RFC 4379 compliant).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 4 | <b>echo revision 4</b><br><br><b>Example:</b><br>Router(config-mpls)# echo revision 4                                                                                                                             | Customizes the default behavior of echo packets. <ul style="list-style-type: none"><li>The <b>revision 4</b> keywords set echo packet attributes to the default Revision 4 (RFC 4379 compliant).</li></ul> <b>Note</b> The MPLS LSP Multipath Tree Trace feature requires Revision 4.                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config-mpls)# end                                                                                                                                                     | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Step 6 | <b>trace mpls multipath ipv4 destination-address/destination-mask-length hashkey ipv4 bitmap bitmap-size</b><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4 10.131.161.251/32 hashkey ipv4 bitmap 16 | Discovers all MPLS LSPs from an egress router to an ingress router. <ul style="list-style-type: none"><li>The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li><li>The <i>destination-address</i> argument is the address prefix of the target to be tested.</li><li>The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The <i>/</i> keyword before this argument is required.</li><li>The <b>hashkey ipv4</b> keywords set the hashkey type to IPv4 addresses.</li><li>The <b>bitmap bitmap-size</b> keyword and arguments set the bitmap size for multipath discovery.</li></ul> |

## Monitoring LSP Paths Discovered by MPLS LSP Multipath Tree Trace Using MPLS LSP Traceroute

Perform the following task to monitor LSP paths discovered by MPLS LSP multipath tree trace using MPLS LSP traceroute. You can take output directly from the **trace mpls multipath** command and add it to a **trace mpls** command periodically to verify that the path is still operating.

Figure 2 shows the mapping of the output of a **trace mpls multipath** command to a **trace mpls** command.

**Figure 2 Mapping of trace mpls multipath Command Output to a trace mpls Command**



Each path you discover with MPLS LSP Multipath Tree Trace can be tested in this manner periodically to monitor the LSP paths in your network.

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* **hashkey** **ipv4** **bitmap** *bitmap-size*
3. **trace mpls ipv4** *destination-address/destination-mask-length* [**output interface** *tx-interface*] [**source** *source-address*] [**destination** *address-start*]
4. **exit**

## DETAILED STEPS

### Step 1 enable

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

```
Router> enable
Router#
```

### Step 2 trace mpls multipath ipv4 destination-address/destination-mask-length hashkey ipv4 bitmap bitmap-size

Use this command to discover all MPLS LSPs from an egress router to an ingress router. For example:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 hashkey ipv4 bitmap 16
```

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,  
 'L' - labeled output interface, 'B' - unlabeled output interface,  
 'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,  
 'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,  
 'P' - no rx intf label prot, 'p' - premature termination of LSP,



```

'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLLL!
Path 0 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
LLL!
Path 1 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
L!
Path 2 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
LL!
Path 3 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7

Paths (found/broken/unexplored) (4/0/0)
Echo Request (sent/fail) (14/0)
Echo Reply (received/timeout) (14/0)
Total Time Elapsed 468 ms

```

The output of the **trace mpls multipath** command in the example shows the result of path discovery with MPLS LSP multipath tree trace. In this example, the command sets the bitmap size to 16. Path discovery starts by MPLS LSP multipath tree trace using 16 bitmapped addresses as it locates LSP paths from the source router to the target router with prefix and mask 10.1.1.150/32. MPLS LSP multipath tree trace starts using the 127.x.y.z/8 address space with 127.0.0.1.

**Step 3** **trace mpls ipv4** *destination-address/destination-mask-length* [**output interface** *tx-interface*] [**source** *source-address*] [**destination** *address-start*]

Use this command to verify that the paths discovered when you entered a **trace mpls multipath** command are still operating. For example, the output for Path 0 in the previous **trace mpls multipath** command in [Step 2](#) is:

```
output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
```

If you put the output for path 0 in the **trace mpls** command, you see the following results:

```
Router# trace mpls ipv4 10.1.1.150/32 output interface Et0/0 source 10.1.111.101
destination 127.0.0.0
```

```
Tracing MPLS Label Switched Path to 10.1.1.150/32, timeout is 2 seconds
```

```

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

```

```

Type escape sequence to abort.
 0 10.1.111.101 MRU 1500 [Labels: 33 Exp: 0]
L 1 10.1.111.111 MRU 1500 [Labels: 34 Exp: 0] 40 ms
L 2 10.2.121.121 MRU 1500 [Labels: 34 Exp: 0] 32 ms
L 3 10.3.132.132 MRU 1500 [Labels: 32 Exp: 0] 16 ms
L 4 10.4.140.240 MRU 1504 [Labels: implicit-null Exp: 0] 20 ms
! 5 10.5.150.50 20 ms

```

You can take output directly from the **trace mpls multipath** command and add it to a **trace mpls** command periodically to verify that the path is still operating (see [Figure 2](#)).

**Step 4    exit**

Use this command to exit to user EXEC mode. for example:

```
Router# exit
Router>
```

---

## Using DSCP to Request a Specific Class of Service in an Echo Reply

For Cisco IOS Release 12.2(27)SXE, Cisco added a reply differentiated services code point (DSCP) option that lets you request a specific class of service (CoS) in an echo reply.

The reply DSCP option is supported in the experimental mode for IETF draft-ietf-mpls-lsp-ping-03.txt. Cisco implemented a vendor-specific extension for the reply DSCP option rather than using a Reply TOS TLV. A Reply TOS TLV serves the same purpose as the **reply dscp** command in IETF draft-ietf-mpls-lsp-ping-11.txt. This draft provides a standardized method of controlling the reply DSCP.

**Note**

Before RFC 4379, Cisco implemented the Reply DSCP option as an experimental capability using a Cisco vendor extension TLV. If a router is configured to encode MPLS echo packets for draft Version 3 implementations, a Cisco vendor extension TLV is used instead of the = Reply TOS TLV that was defined in draft Version 8.

To use DSCP to request a specific CoS in an echo reply, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* [**reply dscp** *dscp-value*]
3. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Step 2 | <b>trace mpls multipath ipv4 destination-address/destination-mask-length [reply dscp dscp-value]</b><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4 10.131.191.252/32 reply dscp 50 | Discovers all MPLS LSPs from an ingress router to an egress router and controls the DSCP value of an echo reply. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The <b>/</b> keyword before this argument is required.</li> <li>The <b>reply dscp dscp-value</b> keywords and argument are the DSCP value of an echo reply. A Reply TOS TLV serves the same purpose as the <b>reply dscp</b> command in IETF draft-ietf-mpls-lsp-ping-11.txt.</li> </ul> <b>Note</b> To specify a DSCP value, you must enter the <b>reply dscp dscp-value</b> keywords and argument. |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                               | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Controlling How a Responding Router Replies to an MPLS Echo Request

This section contains information about and instructions for controlling how a responding router replies to an MPLS echo request. You should understand the following information before you configure a reply mode for the echo request response:

- [Reply Modes for an MPLS LSP Multipath Tree Trace Echo Request Response, page 14](#)

### Reply Modes for an MPLS LSP Multipath Tree Trace Echo Request Response

The reply mode controls how a responding router replies to an MPLS echo request sent by a **trace mpls multipath** command. There are two reply modes for an echo request packet:

- ipv4—Reply with an IPv4 User Datagram Protocol (UDP) packet (default)
- router-alert—Reply with an IPv4 UDP packet with router alert


**Note**

Use the ipv4 and router-alert reply modes with each other to prevent false negatives. If you do not receive a reply via the ipv4 mode, send a test with the router-alert reply mode. If both fail, something is wrong in the return path. The problem might be due to an incorrect ToS setting.

## IPv4 UDP Reply Mode

The IPv4 UDP reply mode is the most common reply mode used with a **trace mpls multipath** command when you want to periodically poll the integrity of an LSP. With this option, you do not have explicit control over whether the packet traverses IP or MPLS hops to reach the originator of the MPLS echo request. If the originating (headend) router fails to receive a reply to an MPLS echo request when you use the **reply mode ipv4** keywords, use the **reply mode router-alert** keywords.

## Router-alert Reply Mode

The router-alert reply mode adds the router alert option to the IP header. When an IP packet that contains an IP router alert option in its IP header or an MPLS packet with a router alert label as its outermost label arrives at a router, the router punts (redirects) the packet to the Route Processor (RP) process level for handling. This forces the RP of each intermediate router to specifically handle the packet at each intermediate hop as it moves back to the destination. Hardware and line-card forwarding inconsistencies are thus bypassed. Router-alert reply mode is slower than IPv4 mode because the reply requires process-level RP handling at each hop.

Table 2 describes how an incoming IP packet with an IP router alert is handled by the router switching path processes when the outgoing packet is an IP packet or an MPLS packet. It also describes how an MPLS packet with a router alert option is handled by the router switching path processes when the outgoing packet is an IP packet or an MPLS packet.

**Table 2** Path Process Handling of IP and MPLS Router Alert Packets

| Incoming Packet                                     | Outgoing Packet                                     | Normal Switching Action                                                                                            | Process Switching Action                                                         |
|-----------------------------------------------------|-----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| IP packet—Router alert option in IP header          | IP packet—Router alert option in IP header          | Router alert option in IP header causes the packet to be punted to the process switching path.                     | Forwards the packet as is                                                        |
|                                                     | MPLS packet                                         |                                                                                                                    | Forwards the packet as is                                                        |
| MPLS packet—Outermost label contains a router alert | IP packet—Router alert option in IP header          | If the router alert label is the outermost label, it causes the packet to be punted to the process switching path. | Removes the outermost router alert label and forwards the packet as an IP packet |
|                                                     | MPLS packet—Outermost label contains a router alert |                                                                                                                    | Preserves the outermost router alert label and forwards the MPLS packet          |

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* **reply mode** {**ipv4** | **router-alert**}
3. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                              | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Step 2 | <b>trace mpls multipath ipv4 destination-address/destination-mask-length reply mode {ipv4   router-alert}</b><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4 10.131.191.252/32 reply mode router-alert | Discovers all MPLS LSPs from an ingress router to an egress router and specifies the reply mode. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>The <b>reply mode</b> keyword requires that you enter one of the following keywords to specify the reply mode: <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword—Reply with an IPv4 UDP packet (default).</li> <li>The <b>router-alert</b> keyword—Reply with an IPv4 UDP packet with router alert.</li> </ul> </li> </ul> <p><b>Note</b> To specify the reply mode, you must enter the <b>reply mode</b> keyword with the <b>ipv4</b> or <b>router-alert</b> keyword.</p> |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                                  | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

## Specifying the Output Interface for Echo Packets Leaving a Router for MPLS LSP Multipath Tree Trace

Perform the following task to specify the output interface for echo packets leaving a router for the MPLS LSP Multipath Tree Trace feature. You can use this task to test the LSPs reachable through a given interface.

### Echo Request Output Interface Control

You can control the interface through which packets leave a router. Path output information is used as input to LSP ping and traceroute.

The echo request output interface control feature allows you to force echo packets through the paths that perform detailed debugging or characterizing of the LSP. This feature is useful if a PE router connects to an MPLS cloud and there are broken links. You can direct traffic through a certain link. The feature also is helpful for troubleshooting network problems.

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* [**output interface** *tx-interface*]
3. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | <b>trace mpls multipath ipv4</b> <i>destination-address/destination-mask-length</i> [ <b>output interface</b> <i>tx-interface</i> ]<br><br><b>Example:</b><br>Router# trace mpls multipath ipv4<br>10.131.159.251/32 output interface ethernet0/0 | Discovers all MPLS LSPs from an ingress router to an egress router and specifies the interface through which echo packets leave a router. <ul style="list-style-type: none"> <li>• The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>• The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>• The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>• The <b>output interface</b> <i>tx-interface</i> keywords and argument specify the output interface for the MPLS echo request.</li> </ul> <b>Note</b> You must specify the <b>output interface</b> keywords. |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                                                                | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Setting the Pace of MPLS Echo Request Packet Transmission for MPLS LSP Multipath Tree Trace

Perform the following task to set the pace of MPLS echo request packet transmission for the MPLS LSP Multipath Tree Trace feature. Echo request traffic pacing allows you to set the pace of the transmission of packets so that the receiving router does not drop packets. If you have a large amount of traffic on your network you might increase the size of the interval to help ensure that the receiving router does not drop packets.

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* [**interval** *milliseconds*]

## 3. exit

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>trace mpls multipath ipv4 destination-address/destination-mask-length [interval milliseconds]</b><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4 10.131.159.251/32 interval 100 | Discovers all MPLS LSPs from an egress router to an ingress router and sets the time in milliseconds between successive MPLS echo requests. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>The <i>destination-mask</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>The <b>interval milliseconds</b> keyword and argument set the time between successive MPLS echo requests in milliseconds. The default is 0 milliseconds.</li> </ul> <b>Note</b> To pace the transmission of packets, you must specify the <b>interval</b> keyword. |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                              | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Enabling MPLS LSP Multipath Tree Trace to Detect LSP Breakages Caused by an Interface That Lacks an MPLS Configuration

Perform the following task to enable MPLS LSP multipath tree trace to detect LSP breakages caused by an interface that lacks an MPLS configuration. If an interface is not configured for MPLS, then it cannot forward MPLS packets.

### Explicit Null Label Shimming Tests LSP Ability to Carry MPLS Traffic

For an MPLS LSP multipath tree trace of LSPs carrying IPv4 FECs, you can force an explicit null label to be added to the MPLS label stack even though the label was unsolicited. This allows MPLS LSP multipath tree trace to detect LSP breakages caused by an interface that is not configured for MPLS. MPLS LSP multipath tree trace does not report that an LSP is functioning when it is unable to send MPLS traffic.

An explicit null label is added to an MPLS label stack if MPLS echo request packets are forwarded from an interface not configured for MPLS that is directly connected to the destination of the MPLS LSP multipath tree trace or if the IP TTL value for the MPLS echo request packets is set to 1.

When you enter a **trace mpls multipath** command, you are looking for all MPLS LSP paths from an egress router to an ingress router. Failure at output interfaces that are not configured for MPLS at the penultimate hop are not detected. Explicit-null shimming allows you to test an LSP's ability to carry MPLS traffic.

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4 destination-address/destination-mask-length force-explicit-null**
3. **exit**

## DETAILED STEP

|        |                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | <b>trace mpls multipath ipv4 destination-address/destination-mask-length force-explicit-null</b><br><br><b>Example:</b><br>Router# trace mpls multipath ipv4<br>10.131.191.252/32 force-explicit-null | Discovers all MPLS LSPs from an egress router to an ingress router and forces an explicit null label to be added to the MPLS label stack. <ul style="list-style-type: none"> <li>• The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>• The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>• The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>• The <b>force-explicit-null</b> keyword forces an explicit null label to be added to the MPLS label stack even though the label was unsolicited.</li> </ul> <p><b>Note</b> You must enter the <b>force-explicit-null</b> keyword to enable MPLS LSP multipath tree trace to detect LSP breakages caused by an interface that is not configured for MPLS.</p> |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                    | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Requesting That a Transit Router Validate the Target FEC Stack for MPLS LSP Multipath Tree Trace

Perform the following task to request that a transit router validate the target FEC stack for the MPLS LSP Multipath Tree Trace feature.

An MPLS echo request tests a particular LSP. The LSP to be tested is identified by the FEC stack.



During an MPLS LSP multipath tree trace, the echo packet validation rules do not require that a transit router validate the target FEC stack TLV. A downstream map TLV containing the correct received labels must be present in the echo request for target FEC stack checking to be performed.

To request that a transit router validate the target FEC stack, set the V flag from the source router by entering the **flags fec** keywords in the **trace mpls multipath** command. The default is that echo request packets are sent with the V flag set to 0.

## SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* [**flags fec**] [**ttl** *maximum-time-to-live*]
3. **exit**

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Step 2 | <b>trace mpls multipath ipv4</b> <i>destination-address/destination-mask-length</i> [ <b>flags fec</b> ] [ <b>ttl</b> <i>maximum-time-to-live</i> ]<br><br><b>Example:</b><br>Router# trace mpls multipath ipv4<br>10.131.159.252/32 flags fec ttl 5 | Discovers all MPLS LSPs from an egress router to an ingress router and requests validation of the target FEC stack by a transit router. <ul style="list-style-type: none"> <li>• The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>• The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>• The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>• The <b>flags fec</b> keywords requests that target FEC stack validation be done at a transit router.</li> <li>• The <b>ttl</b> <i>maximum-time-to-live</i> keyword and argument pair specify a maximum hop count.</li> </ul> <p><b>Note</b> For a transit router to validate the target FEC stack, you must enter the <b>flags fec</b> and <b>ttl</b> keywords.</p> |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                                                                   | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Setting the Number of Timeout Attempts for MPLS LSP Multipath Tree Trace

Perform the following task to set the number of timeout attempts for the MPLS LSP Multipath Tree Trace feature.

A retry is attempted if an outstanding echo request times out waiting for the corresponding echo reply.

### SUMMARY STEPS

1. **enable**
2. **trace mpls multipath ipv4** *destination-address/destination-mask-length* [**retry-count** *retry-count-value*]
3. **exit**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                                                          | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Step 2 | <b>trace mpls multipath ipv4</b> <i>destination-address/destination-mask-length</i> [ <b>retry-count</b> <i>retry-count-value</i> ]<br><br><b>Example:</b><br>Router# trace mpls multipath ipv4 10.131.159.252/32 retry-count 4 | Sets the number of retry attempts during an MPLS LSP multipath tree trace. <ul style="list-style-type: none"> <li>• The <b>ipv4</b> keyword specifies the destination type as an LDP IPv4 address.</li> <li>• The <i>destination-address</i> argument is the address prefix of the target to be tested.</li> <li>• The <i>destination-mask-length</i> argument is the number of bits in the network mask of the target address. The / keyword before this argument is required.</li> <li>• The <b>retry-count</b> <i>retry-count-value</i> keyword and argument sets the number of retry attempts after a timeout occurs.</li> </ul> <p>A rertry-count value of “0” means infinite retries. A retry-count value from 0 to10 is suggested. You might want to increase the retry value to greater than 10, if 10 is too small a value. The default retry-count value is 3.</p> <p><b>Note</b> To set the number of retries after a timeout, you must enter the <b>retry-count</b> keyword.</p> |
| Step 3 | <b>exit</b><br><br><b>Example:</b><br>Router# exit                                                                                                                                                                              | Returns to user EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

# Configuration Examples for MPLS EM—MPLS LSP Multipath Tree Trace

This section includes the following configuration examples for the MPLS EM—MPLS LSP Multipath Tree Trace feature:

- [Customizing the Default Behavior of MPLS Echo Packets: Example, page 22](#)
- [Configuring MPLS LSP Multipath Tree Trace: Example, page 22](#)
- [Using DSCP to Request a Specific Class of Service in an Echo Reply: Example, page 24](#)
- [Controlling How a Responding Router Replies to an MPLS Echo Request: Example, page 25](#)
- [Specifying the Output Interface for Echo Packets Leaving a Router for MPLS LSP Multipath Tree Trace: Example, page 25](#)
- [Setting the Pace of MPLS Echo Request Packet Transmission for MPLS LSP Multipath Tree Trace: Example, page 26](#)
- [Enabling MPLS LSP Multipath Tree Trace to Detect LSP Breakages Caused by an Interface That Lacks an MPLS Configuration: Example, page 27](#)
- [Requesting That a Transit Router Validate the Target FEC Stack for MPLS LSP Multipath Tree Trace: Example, page 29](#)
- [Setting the Number of Timeout Attempts for MPLS LSP Multipath Tree Trace: Example, page 29](#)

## Customizing the Default Behavior of MPLS Echo Packets: Example

The following example shows how to customize the behavior of MPLS echo packets so that the MPLS LSP Multipath Tree Trace feature interoperates with a vendor implementation that does not interpret RFC 4379 as Cisco does:

```
configure terminal
!
mpls oam
 echo revision 4
no echo vendor-extension
end
```

The **echo revision** command is included in this example for completeness. The default echo revision number is 4, which corresponds to RFC 4379.

## Configuring MPLS LSP Multipath Tree Trace: Example

The following example shows how to configure the MPLS LSP Multipath Tree Trace feature to interoperate with a vendor implementation that does not interpret RFC 4379 as Cisco does:

```
configure terminal
!
mpls oam
 echo revision 4
no echo vendor-extension
end
!
trace mpls multipath ipv4 10.131.161.151/32
```

The **echo revision** command is included in this example for completeness. The default echo revision number is 4, which corresponds to the RFC 4379.

## Discovering IPv4 Load Balancing Paths Using MPLS LSP Multipath Tree Trace: Example

The following example shows how to use the MPLS LSP Multipath Tree Trace feature to discover IPv4 load balancing paths. The example is based on the sample network shown in [Figure 3](#). In this example, the bitmap size is set to 16. Therefore, path discovery starts by the MPLS LSP Multipath Tree Trace feature using 16 bitmapped addresses as it locates LSP paths from the source router R-101 to the target router R-150 with prefix and mask 10.1.1.150/32. The MPLS LSP Multipath Tree Trace feature starts using the 127.x.y.z/8 address space with 127.0.0.0.

```
Router# trace mpls multipath ipv4 10.1.1.150/32 hashkey ipv4 bitmap 16
```

```
Starting LSP Multipath Traceroute for 10.1.1.150/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
LLLL!
```

```
Path 0 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
```

```
LLL!
```

```
Path 1 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
```

```
L!
```

```
Path 2 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
```

```
LL!
```

```
Path 3 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
```

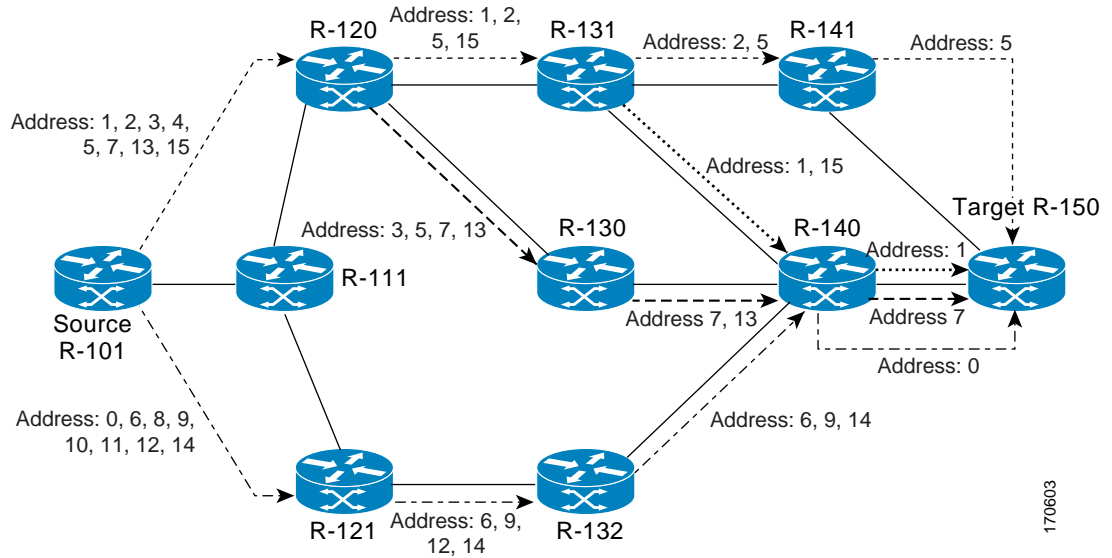
```
Paths (found/broken/unexplored) (4/0/0)
```

```
Echo Request (sent/fail) (14/0)
```

```
Echo Reply (received/timeout) (14/0)
```

```
Total Time Elapsed 468 ms
```

The output of the **trace mpls multipath** command in the example shows the result of path discovery with the MPLS LSP Multipath Tree Trace feature as shown in [Figure 3](#).

**Figure 3** *MPLS LSP Multipath Tree Trace Path Discovery in a Sample Network*

## Using DSCP to Request a Specific Class of Service in an Echo Reply: Example

The following example shows how to use DSCP to request a specific CoS in an echo reply:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 reply dscp 50
```

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,  
 'L' - labeled output interface, 'B' - unlabeled output interface,  
 'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,  
 'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,  
 'P' - no rx intf label prot, 'p' - premature termination of LSP,  
 'R' - transit router, 'I' - unknown upstream index,  
 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

LLLL!

Path 0 found,

output interface Et0/0 source 10.1.111.101 destination 127.0.0.0

LLL!

Path 1 found,

output interface Et0/0 source 10.1.111.101 destination 127.0.0.1

L!

Path 2 found,

output interface Et0/0 source 10.1.111.101 destination 127.0.0.5

LL!

Path 3 found,

output interface Et0/0 source 10.1.111.101 destination 127.0.0.7

Paths (found/broken/unexplored) (4/0/0)

Echo Request (sent/fail) (14/0)

Echo Reply (received/timeout) (14/0)

Total Time Elapsed 448 ms

170603

## Controlling How a Responding Router Replies to an MPLS Echo Request: Example

The following example shows how to control how a responding router replies to an MPLS echo request:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 reply mode router-alert
```

```
Starting LSP Multipath Traceroute for 10.1.1.150/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
LLLL!
```

```
Path 0 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
```

```
LLL!
```

```
Path 1 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
```

```
L!
```

```
Path 2 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
```

```
LL!
```

```
Path 3 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
```

```
Paths (found/broken/unexplored) (4/0/0)
```

```
Echo Request (sent/fail) (14/0)
```

```
Echo Reply (received/timeout) (14/0)
```

```
Total Time Elapsed 708 ms
```

## Specifying the Output Interface for Echo Packets Leaving a Router for MPLS LSP Multipath Tree Trace: Example

The following example shows how to specify the output interface for echo packets leaving a router for the MPLS LSP Multipath Tree Trace feature:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 output interface ethernet0/0
```

```
Tracing MPLS Label Switched Path to 10.1.1.150/32, timeout is 2 seconds
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
  0 10.1.111.101 MRU 1500 [Labels: 33 Exp: 0]
```

```
L
```

```
  1 10.1.111.111 MRU 1500 [Labels: 33 Exp: 0] 40 ms
```

```
L
```

```

2 10.2.120.120 MRU 1500 [Labels: 33 Exp: 0] 20 ms
L
3 10.3.131.131 MRU 1500 [Labels: 34 Exp: 0] 20 ms
L
4 10.4.141.141 MRU 1504 [Labels: implicit-null Exp: 0] 20 ms !
5 10.5.150.150 16 ms

```

## Setting the Pace of MPLS Echo Request Packet Transmission for MPLS LSP Multipath Tree Trace: Example

The following examples show how set the pace of MPLS echo request packet transmission for the MPLS LSP Multipath Tree Trace feature. The time between successive MPLS echo requests is set to 300 milliseconds in the first example and 400 milliseconds in the second example:

```
Router# trace mpls multipath ipv4 10.131.159.252/32 interval 300
```

```
Starting LSP Multipath Traceroute for 10.131.159.252/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

```

```
Type escape sequence to abort.
```

```
LL!
```

```
Path 0 found,
output interface Et1/0 source 10.2.3.2 destination 127.0.0.0

```

```
Paths (found/broken/unexplored) (1/0/0)
Echo Request (sent/fail) (3/0)
Echo Reply (received/timeout) (3/0)
Total Time Elapsed 1604 ms

```

```
Router# trace mpls multipath ipv4 10.131.159.252/32 interval 400
```

```
Starting LSP Multipath Traceroute for 10.131.159.252/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

```

```
Type escape sequence to abort.
```

```
LL!
```

```
Path 0 found,
output interface Et1/0 source 10.2.3.2 destination 127.0.0.0

```

```
Paths (found/broken/unexplored) (1/0/0)
Echo Request (sent/fail) (3/0)
Echo Reply (received/timeout) (3/0)
Total Time Elapsed 1856 ms

```

Notice that the elapsed time increases as you increase the interval size.

## Enabling MPLS LSP Multipath Tree Trace to Detect LSP Breakages Caused by an Interface That Lacks an MPLS Configuration: Example

The following examples shows how to enable the MPLS LSP Multipath Tree Trace feature to detect LSP breakages caused by an interface that lacks an MPLS configuration:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 force-explicit-null
```

```
Starting LSP Multipath Traceroute for 10.1.1.150/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
LLLL!
```

```
Path 0 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
```

```
LLL!
```

```
Path 1 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
```

```
L!
```

```
Path 2 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
```

```
LL!
```

```
Path 3 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
```

```
Paths (found/broken/unexplored) (4/0/0)
```

```
Echo Request (sent/fail) (14/0)
```

```
Echo Reply (received/timeout) (14/0)
```

```
Total Time Elapsed 460 ms
```

This example shows the additional information provided when you add the **verbose** keyword to the command:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 force-explicit-null verbose
```

```
Starting LSP Multipath Traceroute for 10.1.1.150/32
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
LLLL!
```

```
Path 0 found,
```

```
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
```

```
    0 10.1.111.101 10.1.111.111 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] multipaths 0
```

```
L
```

```
    1 10.1.111.111 10.2.121.121 MRU 1500 [Labels: 34/explicit-null Exp: 0/0] ret code 8
```

```
  multipaths 2
```

```
L
```



```

    2 10.2.121.121 10.3.132.132 MRU 1500 [Labels: 34/explicit-null Exp: 0/0] ret code 8
multipaths 1
L
    3 10.3.132.132 10.4.140.240 MRU 1500 [Labels: 32/explicit-null Exp: 0/0] ret code 8
multipaths 1
L
    4 10.4.140.240 10.5.150.50 MRU 1504 [Labels: explicit-null Exp: 0] ret code 8 multipaths
1 !
    5 10.5.150.50, ret code 3 multipaths 0
LLL!
Path 1 found,
output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
    0 10.1.111.101 10.1.111.111 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] multipaths 0
L
    1 10.1.111.111 10.2.120.120 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    2 10.2.120.120 10.3.131.131 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    3 10.3.131.131 10.4.141.141 MRU 1500 [Labels: 34/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    4 10.4.141.141 10.5.150.150 MRU 1504 [Labels: explicit-null Exp: 0] ret code 8
multipaths 1
!
    5 10.5.150.150, ret code 3 multipaths 0
L!
Path 2 found,
output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
    0 10.1.111.101 10.1.111.111 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] multipaths 0
L
    1 10.1.111.111 10.2.120.120 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    2 10.2.120.120 10.3.131.131 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    3 10.3.131.131 10.4.140.140 MRU 1500 [Labels: 32/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    4 10.4.140.140 10.5.150.50 MRU 1504 [Labels: explicit-null Exp: 0] ret code 8 multipaths
1 ! 5 10.5.150.50, ret code 3 multipaths 0
LL!
Path 3 found,
output interface Et0/0 source 10.1.111.101 destination 127.0.0.7
    0 10.1.111.101 10.1.111.111 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] multipaths 0
L
    1 10.1.111.111 10.2.120.120 MRU 1500 [Labels: 33/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    2 10.2.120.120 10.3.130.130 MRU 1500 [Labels: 34/explicit-null Exp: 0/0] ret code 8
multipaths 2
L
    3 10.3.130.130 10.4.140.40 MRU 1500 [Labels: 32/explicit-null Exp: 0/0] ret code 8
multipaths 1
L
    4 10.4.140.40 10.5.150.50 MRU 1504 [Labels: explicit-null Exp: 0] ret code 8 multipaths
1
!
    5 10.5.150.50, ret code 3 multipaths 0

Paths (found/broken/unexplored) (4/0/0)
Echo Request (sent/fail) (14/0)

```

```
Echo Reply (received/timeout) (14/0)
Total Time Elapsed 492 ms
```

## Requesting That a Transit Router Validate the Target FEC Stack for MPLS LSP Multipath Tree Trace: Example

The following example shows how to request that a transit router validate the target FEC stack for the MPLS LSP Multipath Tree Trace feature:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 flags fec ttl 5

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'I' - unknown upstream index,
        'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLLL!
Path 0 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
LLL!
Path 1 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
L!
Path 2 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
LL!
Path 3 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7

Paths (found/broken/unexplored) (4/0/0)
Echo Request (sent/fail) (14/0)
Echo Reply (received/timeout) (14/0)
Total Time Elapsed 464 ms
```

Target FEC stack validation is always done at the egress router when the **flags fec** keywords are specified in the **trace mpls multipath** command.

## Setting the Number of Timeout Attempts for MPLS LSP Multipath Tree Trace: Example

The following example sets the number of timeout attempts for the MPLS LSP Multipath Tree Trace feature to four:

```
Router# trace mpls multipath ipv4 10.1.1.150/32 retry-count 4

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
```

```

'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLL!
Path 0 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
LLL!
Path 1 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1
L!
Path 2 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.5
LL!
Path 3 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7

Paths (found/broken/unexplored) (4/0/0)
Echo Request (sent/fail) (14/0)
Echo Reply (received/timeout) (14/0)
Total Time Elapsed 460 ms

```

The following output shows a **trace mpls multipath** command that found one unexplored path, one successful path, and one broken path:

```

Router# trace mpls multipath ipv4 10.1.1.150/32 retry-count 4

Starting LSP Multipath Traceroute for 10.1.1.150/32

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
LLL....
Path 0 Unexplorable,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.0
LLL!
Path 1 found,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.1 B
Path 2 Broken,
  output interface Et0/0 source 10.1.111.101 destination 127.0.0.7

Paths (found/broken/unexplored) (1/1/1)
Echo Request (sent/fail) (12/0)
Echo Reply (received/timeout) (8/4)
Total Time Elapsed 7868 ms

```

# Additional References

The following sections provide references related to the MPLS EM—MPLS LSP Multipath Tree Trace feature.

## Related Documents

| Related Topic                                                    | Document Title                                                              |
|------------------------------------------------------------------|-----------------------------------------------------------------------------|
| Concepts and configuration tasks for MPLS LSP ping or traceroute | <a href="#">MPLS Embedded Management—LSP Ping/Traceroute and AToM VCCV</a>  |
| Concepts and configuration for MPLS and other MPLS applications  | <a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a> |
| MPLS commands                                                    | <a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>   |
| Troubleshooting procedures for MPLS                              | <a href="#">Cisco—MPLS Troubleshooting</a>                                  |

## Standards

| Standard                                                                                                                              | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIB                                                                                                                         | MIBs Link                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

## RFCs

| RFC      | Title                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------|
| RFC 2113 | <i>IP Router Alert Option</i>                                                                         |
| RFC 3443 | <i>Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks</i>                |
| RFC 4377 | <i>Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks</i> |
| RFC 4378 | <i>A Framework for Multi-Protocol Label Switching (MPLS) Operations and Management (OAM)</i>          |
| RFC 4379 | <i>Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures</i>                             |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **debug mpls lspv**
- **echo**
- **mpls oam**
- **trace mpls**
- **trace mpls multipath**

# Feature Information for MPLS EM—MPLS LSP Multipath Tree Trace

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for MPLS EM—MPLS LSP Multipath Tree Trace

| Feature Name                          | Releases                                               | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MPLS EM—MPLS LSP Multipath Tree Trace | 12.2(31)SB2<br>12.2(33)SRB<br>12.4(20)T<br>12.2(33)SXI | <p>The MPLS EM—MPLS LSP Multipath Tree Trace feature provides the means to discover all the possible paths of a label switched path (LSP) between an egress and ingress router. Once discovered, these paths can be retested on a periodic basis using Multiprotocol Label Switching (MPLS) LSP ping or traceroute. This feature is an extension to the MPLS LSP traceroute functionality for the tracing of IPv4 LSPs.</p> <p>Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.</p> <p>In Cisco IOS Release 12.2(31)SB2, this feature was introduced.</p> <p>In Cisco IOS Release 12.2(33)SRB, support was added for a Cisco IOS 12.2SR release.</p> <p>In Cisco IOS Release 12.(20)T, support was added for a Cisco IOS 12.4T release.</p> <p>In Cisco IOS Release 12.2(33)SXI, support was added for a Cisco IOS 12.2SX release.</p> |

**Table 3**      **Feature Information for MPLS EM—MPLS LSP Multipath Tree Trace (continued)**

| Feature Name | Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|              |          | <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Overview of MPLS LSP Multipath Tree Trace, page 3</a></li> <li>• <a href="#">Discovery of IPv4 Load Balancing Paths by MPLS LSP Multipath Tree Trace, page 3</a></li> <li>• <a href="#">Echo Reply Return Codes Sent by the Router Processing Multipath LSP Tree Trace, page 4</a><a href="#">Customizing the Default Behavior of MPLS Echo Packets, page 5</a></li> <li>• <a href="#">Configuring MPLS LSP Multipath Tree Trace, page 7</a></li> <li>• <a href="#">Discovering IPv4 Load Balancing Paths Using MPLS LSP Multipath Tree Trace, page 9</a><a href="#">Monitoring LSP Paths Discovered by MPLS LSP Multipath Tree Trace Using MPLS LSP Traceroute, page 10</a></li> <li>• <a href="#">Using DSCP to Request a Specific Class of Service in an Echo Reply, page 13</a></li> <li>• <a href="#">Controlling How a Responding Router Replies to an MPLS Echo Request, page 14</a></li> <li>• <a href="#">Specifying the Output Interface for Echo Packets Leaving a Router for MPLS LSP Multipath Tree Trace, page 16</a></li> <li>• <a href="#">Setting the Pace of MPLS Echo Request Packet Transmission for MPLS LSP Multipath Tree Trace, page 17</a></li> <li>• <a href="#">Enabling MPLS LSP Multipath Tree Trace to Detect LSP Breakages Caused by an Interface That Lacks an MPLS Configuration, page 18</a></li> <li>• <a href="#">Requesting That a Transit Router Validate the Target FEC Stack for MPLS LSP Multipath Tree Trace, page 19</a></li> <li>• <a href="#">Setting the Number of Timeout Attempts for MPLS LSP Multipath Tree Trace, page 21</a></li> </ul> <p>The following commands were introduced or modified:<br/> <b>debug mpls lsvp, echo, mpls oam, trace mpls, trace mpls multipath.</b></p> |

# Glossary

**ECMP**—equal-cost multipath. Multiple routing paths of equal cost that may be used for packet forwarding.

**FEC**—Forwarding Equivalence Class. A set of packets that can be handled equivalently for forwarding purposes and are thus suitable for binding to a single label. Examples include the set of packets destined for one address prefix and the packets in any flow.

**flow**—A set of packets traveling between a pair of hosts, or between a pair of transport protocol ports on a pair of hosts. For example, packets with the same source address, source port, destination address, and destination port might be considered a flow.

A flow is also a stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

**localhost**—A name that represents the host router (device). The localhost uses the reserved loopback IP address 127.0.0.1.

**LSP**—label switched path. A connection between two routers in which MPLS forwards the packets.

**LSPV**—Label Switched Path Verification. An LSP ping subprocess. It encodes and decodes MPLS echo requests and replies, and it interfaces with IP, MPLS, and AToM switching for sending and receiving MPLS echo requests and replies. At the MPLS echo request originator router, LSPV maintains a database of outstanding echo requests for which echo responses have not been received.

**MPLS router alert label**—An MPLS label of 1. An MPLS packet with a router alert label is redirected by the router to the Route Processor (RP) processing level for handling. This allows these packets to bypass any forwarding failures in hardware routing tables.

**OAM**—Operation, Administration, and Management.

**punt**—Redirect packets with a router alert from the line card or interface to Route Processor (RP) level processing for handling.

**RP**—Route Processor. The processor module in a Cisco 7000 series router that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**TTL**—time-to-live. A parameter you can set that indicates the maximum number of hops a packet should take to reach its destination.

**TLV**—type, length, values. A block of information included in a Cisco Discovery Protocol address.

**UDP**—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, so error processing and retransmission must be handled by other protocols. UDP is defined in RFC 768.

**XDR**—eXternal Data Representation. Standard for machine-independent data structures developed by Sun Microsystems. Used to transport messages between the Route Processor (RP) and the line card.



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

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

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

© 2006–2009 Cisco Systems, Inc. All rights reserved.



# MPLS Enhancements to Interfaces MIB

---

**First Published: March 15, 2004**

**Last Updated: April 18, 2008**

This document describes the Multiprotocol Label Switching (MPLS) enhancements to the existing Interfaces MIB (RFC 2233) to support an MPLS layer. This layer provides counters and statistics specifically for MPLS.

## History for MPLS Enhancements to Interfaces MIB Feature

| Release     | Modification                                                    |
|-------------|-----------------------------------------------------------------|
| 12.0(23)S   | This feature was introduced.                                    |
| 12.3(8)T    | This feature was integrated into Cisco IOS Release 12.3(8)T.    |
| 12.2(33)SRA | This feature was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This feature was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SB  | This feature was integrated into Cisco IOS Release 12.2(33)SB.  |

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS Enhancements to Interfaces MIB, page 2](#)
- [Restrictions for MPLS Enhancements to Interfaces MIB, page 2](#)
- [Information About MPLS Enhancements to Interfaces MIB, page 3](#)
- [How to Configure MPLS Enhancements to Interfaces MIB, page 8](#)
- [Configuration Examples for the MPLS Enhancements to Interfaces MIB, page 10](#)
- [Additional References, page 10](#)
- [Command Reference, page 12](#)



---

**Americas Headquarters:**

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

© 2004–2008 Cisco Systems, Inc. All rights reserved.

- [Glossary, page 13](#)

## Prerequisites for MPLS Enhancements to Interfaces MIB

- SNMP must be installed and enabled on the label switching routers (LSRs)
- MPLS must be enabled on the LSRs
- MPLS IP must be enabled on an interface or an MPLS traffic engineering (TE) tunnel enabled on an interface

## Restrictions for MPLS Enhancements to Interfaces MIB

- Link up and link down traps for the MPLS layer are not supported in this release. Link up and link down traps for the MPLS layer are supported in Cisco IOS Releases 12.2(33)SXH, 12.2(33)SB, 12.2(33)SRB and later releases.
- Write capability using the SNMP SET command is not supported for the MPLS layer in this release.
- Some counters, including discard and multicast, increment on the underlying physical layer; therefore, they equal 0 because they never reach the MPLS layer.
- Starting in Cisco IOS Release 12.4, the high-capacity counters for the MPLS layer interfaces of the Interfaces MIB contain 64 bits of counter data. In previous releases, the high capacity counters displayed 32 bits of counter data.

The following MIB objects are affected:

- ifHCInOctets
- ifHCOctets
- ifHCInUcastPkts
- ifHCOctetsUcastPkts

When the 64-bit values are less than the value of 232, the 32-bit and 64-bit values are identical.

After the counter increases to more than 232, the counters are different; the 64-bit value is computed by the following formula:

$$X * (232) + Y$$

where:

- X is the number of times the 32-bit counter has rolled.
- Y is the residual value of the counter after the roll occurred. The Y value equals the 32-bit value.

When the high-capacity counter values are compared to their 32-bit values, there is a period of time that the counter values are not equal. The 64-bit values lag the 32-bit values when the counters poll the 32-bit hardware counters and computing the correct counter value. During the polling and computation interval, the following high-capacity counter values counters might be inconsistent:

- ifInOctets
- ifOutOctets
- ifInUcastPkts
- ifOutUcastPkts

The inconsistent values can occur if traffic is constantly flowing over an interface and a MIB walk is performed. The 32-bit value is correct at that moment. The 64-bit value lags slightly, because of the polling computations needed to generate it. Once traffic stops flowing over the interface, and a polling period has passed, the two counters are identical and correct.

The lag time depends on the following factors:

- The polling interval used by the Interfaces MIB. The less time the polling interval takes, the more accurate the value is.
- The size of the Interfaces MIB. A large MIB takes a long time to walk and might affect the values found at that instant.
- The number of computations needed to generate the 64-bit value. The number of MPLS-enabled interfaces increases the number of 64-bit counter values that need to be computed.

## Information About MPLS Enhancements to Interfaces MIB

To configure the MPLS Enhancements to Interfaces MIB, you need to understand the following concepts:

- [Feature Design of the MPLS Enhancements to Interfaces MIB, page 3](#)
- [Interfaces MIB Scalar Objects, page 5](#)
- [Stacking Relationships for MPLS Layer Interfaces, page 5](#)
- [Stacking Relationships for Traffic Engineering Tunnels, page 6](#)
- [MPLS Label Switching Router MIB Enhancements, page 7](#)
- [Benefits of the MPLS Enhancements to Interfaces MIB, page 8](#)

## Feature Design of the MPLS Enhancements to Interfaces MIB

The Interfaces MIB (IF MIB) provides an SNMP-based method for managing interfaces. Each entry in the IF MIB establishes indexing, statistics, and stacking relationships among underlying physical interfaces, subinterfaces, and Layer 2 protocols that exist within Cisco IOS software.

The enhancements add an MPLS layer to the IF MIB as a Layer 2 protocol to provide statistics for traffic encapsulated as MPLS on an interface. In this structure, MPLS-specific data such as MPLS-encapsulated traffic counters and the MPLS maximum transmission unit (MTU) resides on top of the underlying physical or virtual interface to allow separation from non-MPLS data.

The enhancements also allow you to display indexing, statistics, and stacking relationships using the `ifStackTable`. MPLS layer interfaces are stacked above the underlying physical or virtual interface that is actually forwarding the MPLS traffic. MPLS traffic engineering tunnels are then stacked above those MPLS layers.

The IF MIB supports several types of interfaces. A virtual interface that provides protocol statistics for MPLS-encapsulated traffic has been added. This interface is stacked above real Cisco IOS interfaces or subinterfaces, such as Ethernet (et0) or ATM (at1/1.1).

Cisco IOS software creates a corresponding MPLS layer above each interface capable of supporting MPLS when the MPLS encapsulation is enabled by issuing the **mpls ip** interface configuration command.

You can also create the interface layer if you enable MPLS TE by using the **mpls traffic-eng tunnels** command in interface configuration mode.

**Note**

You must also issue these commands in global configuration mode for MPLS IP or MPLS TE to be enabled.

An IF MIB entry is created when you enable either MPLS IP or MPLS TE tunnels on an interface; the entry is removed when you disable both MPLS IP and MPLS TE.

## ifStackTable Objects

Table 1 defines the ifStackTable objects.

**Table 1** *ifStackTable Objects and Definitions*

| Object             | Definition                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ifStackHigherLayer | <p>The value of ifIndex corresponding to the higher sublayer of the relationship; that is, the sublayer that runs on top of the sublayer identified by the corresponding instance of the ifStackLowerLayer.</p> <p><b>Note</b> Index objects are not accessible in a MIB walk. This value is part of the object identifier (OID) for every object in the ifStackTable.</p> |
| ifStackLowerLayer  | <p>The value of ifIndex corresponding to the lower sublayer of the relationship; that is, the sublayer that runs below the sublayer identified by the corresponding instance of the ifStackHigherLayer.</p> <p><b>Note</b> Index objects are not accessible in a MIB walk. This value is part of the OID for every object in the ifStackTable.</p>                         |
| ifStackStatus      | Used to create and delete rows in the ifStackTable; status is always active(1) for MPLS.                                                                                                                                                                                                                                                                                   |

## ifRcvAddressTable Objects

Table 2 defines the ifRcvAddressTable objects.

**Note**

Entries for the MPLS layer do not appear in the ifRcvAddressTable.

**Table 2** *ifRcvAddressTable Objects and Descriptions*

| Object              | Definition                                                                                                                                                                                                                        |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ifRcvAddressAddress | An address for which the system accepts packets and frames on this entry's interface.<br><br><b>Note</b> Index objects are not accessible in a MIB walk. This value is part of the OID for every object in the ifRcvAddressTable. |
| ifRcvAddressStatus  | Used to create and delete rows in the ifRcvAddressTable.                                                                                                                                                                          |
| ifRcvAddressType    | Type of storage used for each entry in the ifRcvAddressTable.                                                                                                                                                                     |

## Interfaces MIB Scalar Objects

The IF MIB supports the following scalar objects:

- **ifStackLastChange**—The value of sysUpTime at the time of the last change of the entire interface stack. A change of the interface stack is defined to be any creation, deletion, or change in value of any instance of ifStackStatus. If the interface stack has been unchanged since the last reinitialization of the local network management subsystem, then this object contains a zero value.
- **ifTableLastChange**—The value of sysUpTime at the time of the last creation or deletion of an entry in the ifTable. If the number of entries has been unchanged since the last reinitialization of the local network management subsystem, then this object contains a zero value.

## Stacking Relationships for MPLS Layer Interfaces

The ifStackTable within the IF MIB provides a conceptual stacking relationship between the interfaces and subinterfaces represented as entries in the ifTable.

The ifStackTable is indexed like a linked list. Each entry shows a relationship between two interfaces providing the ifIndexes of the upper and the lower interface. The entries chain together to show the entire stacking relationship. Each entry links with one another until the stack terminates with an ifIndex of 0 at the highest and lowest ends of the stack. For example, in [Figure 1](#), the indexes .10.5 show that ifIndex 10 is stacked upon ifIndex 5. There are 0 entries at the highest and lowest ends of the stack; in [Figure 1](#), the indexes .0.15 and .72.0 are the highest and lowest ends of the stack, respectively.

Figure 1 Sample ATM Stacking Relationship in the ifStackTable

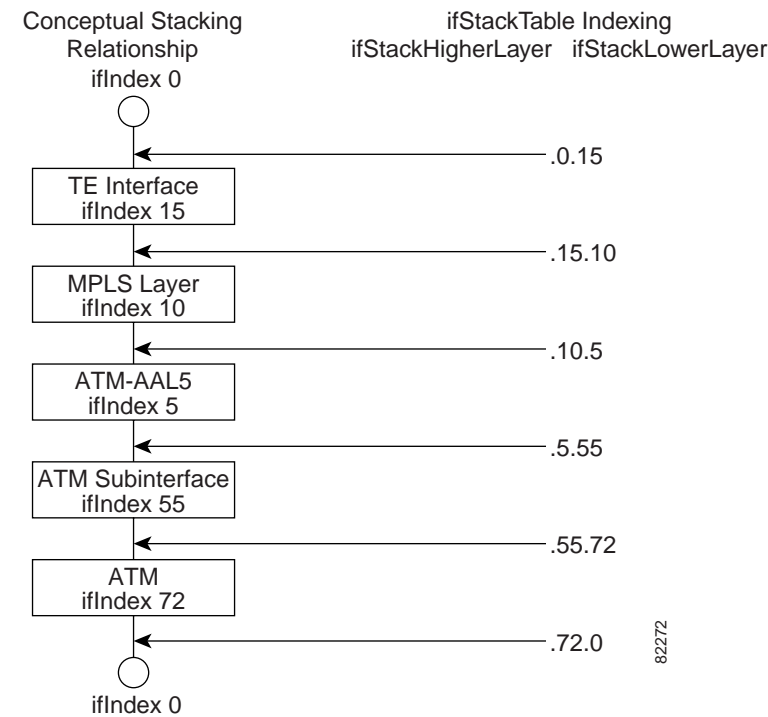


Table 3 describes the indexing of the ifStackTable for the layer relationships shown in Figure 1.



Note

The order of the entries in Table 3 may not be the same as that seen in the MIB walk, which has to follow SNMP ordering rules.

Table 3 Layer Relationships

| Layer Relationship (in Descending Order)     | ifStackHigherLayer/ifStackLowerLayer |
|----------------------------------------------|--------------------------------------|
| TE interface as top layer                    | .0.15                                |
| TE interface stacked upon MPLS layer         | .15.10                               |
| MPLS layer stacked upon ATM-AAL5             | .10.5                                |
| ATM-AAL5 layer stacked upon ATM subinterface | .5.55                                |
| ATM subinterface stacked upon ATM            | .55.72                               |
| ATM as bottom layer                          | .72.0                                |

## Stacking Relationships for Traffic Engineering Tunnels

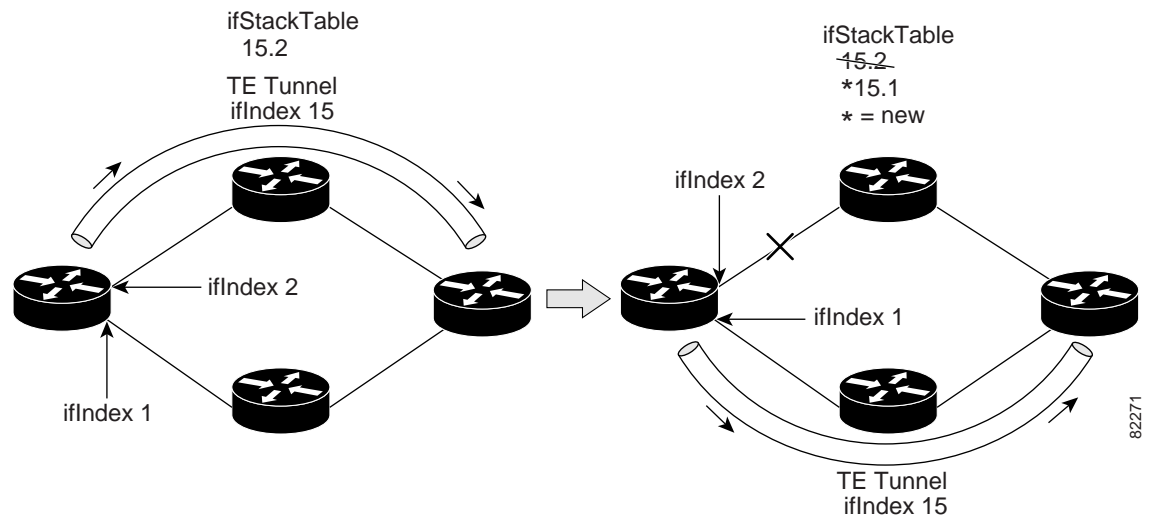
MPLS TE tunnels are represented in Cisco IOS software and the IF MIB as virtual interfaces. When properly signaled, TE tunnels pass traffic through MPLS over a physical interface. This process dictates that a TE tunnel is to be stacked on an MPLS layer that is stacked on an underlying interface.

TE tunnels can also change paths in response to different error or network conditions. These changes are instigated by using the RSVP-TE signaling protocol. When a change occurs, a tunnel can switch to a different MPLS interface. If no signaling path exists, no paths will be chosen and thus no MPLS interface will be used.

Because a TE tunnel is represented as an IF MIB ifTable entry, the ifStackTable also contains an entry corresponding to the TE tunnel. If the TE tunnel is successfully signaled, the ifStackTable also contains a link between the tunnel interface and one MPLS interface. Note that because it is possible for a TE tunnel to not have a corresponding signaled path, it is thus possible for a TE tunnel's ifStackTable entry to not have a corresponding lower layer. In this case, the lower layer variable contains the value of 0.

Figure 2 shows a TE tunnel before (left) and after (right) being rerouted and the effect on the ifStackTable. When ifIndex 2 fails, the TE tunnel is rerouted through ifIndex 1, the 15.2 entry is removed from the ifStackTable, and the 15.1 entry is added.

**Figure 2** Sample TE Tunnel Stacking Relationship



## MPLS Label Switching Router MIB Enhancements

All of the ifIndex references in the MPLS-LSR-MIB tables have changed from the ifIndex of the underlying physical or virtual interface to the ifIndex of the MPLS layer.

Table 4 shows the specific changes.

**Table 4** MPLS-LSR-MIB ifIndex Objects Enhanced

| Table                                                       | ifIndex                |
|-------------------------------------------------------------|------------------------|
| MPLS interface configuration table (mplsInterfaceConfTable) | mplsInterfaceConfIndex |
| MPLS in-segment table (mplsInSegmentTable)                  | mplsInSegmentIfIndex   |
| MPLS cross-connect table (mplsXCTable)                      | mplsInSegmentIfIndex   |
| MPLS out-segment table (mplsOutSegmentTable)                | mplsOutSegmentIfIndex  |

The following objects from the mplsInterfaceConfTable are affected:



- `mplsInterfaceOutPackets`—Count only MPLS-encapsulated out packets
- `mplsInterfaceInPackets`—Count only MPLS-encapsulated in packets

## Benefits of the MPLS Enhancements to Interfaces MIB

### Improved Accounting Capability

By viewing the MPLS layer, you get MPLS-encapsulated traffic counters that do not include non-MPLS encapsulated traffic (for example, IP packets). Therefore, the counters are more useful for MPLS-related statistics.

### TE Tunnel Interfaces

For TE tunnel interfaces, the stacking relationship reflects the current underlying MPLS interface that is in use and dynamically changes as TE tunnels reoptimize and reroute.

### MPLS-Specific Information

The MPLS layer shows MPLS-specific information including the following:

- If MPLS is enabled
- MPLS counters
- MPLS MTU
- MPLS operational status

## How to Configure MPLS Enhancements to Interfaces MIB

This section contains the following procedures:

- [Enabling the SNMP Agent, page 8](#) (required)
- [Configuration Examples for the MPLS Enhancements to Interfaces MIB, page 10](#) (optional)

## Enabling the SNMP Agent

Perform the following task to enable the SNMP agent.

### SUMMARY STEPS

1. `enable`
2. `show running-config`
3. `configure terminal`
4. `snmp-server community string [view view-name] [ro] [number]`
5. `end`
6. `write memory`

## DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                |
| Step 2 | <b>show running-config</b><br><br><b>Example:</b><br>Router# show running-config                                                                                                      | Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.<br><br>If no SNMP information is displayed, continue with the next step.<br><br>If any SNMP information is displayed, you can modify the information or change it as desired.                                                                                                     |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                               |
| Step 4 | <b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b> ] [ <i>number</i> ]<br><br><b>Example:</b><br>Router(config)# snmp-server community public ro | Configures read-only (ro) community strings for the MPLS Label Distribution Protocol (LDP) MIB. <ul style="list-style-type: none"> <li>The <i>string</i> argument functions like a password, permitting access to SNMP functionality on label switch routers (LSRs) in an MPLS network.</li> <li>The optional <b>ro</b> keyword configures read-only (ro) access to the objects in the MPLS LDP MIB.</li> </ul> |
| Step 5 | <b>end</b><br><br><b>Example:</b><br>Router(config)# end                                                                                                                              | Exits to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                  |
| Step 6 | <b>write memory</b><br><br><b>Example:</b><br>Router# write memory                                                                                                                    | Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.                                                                                                                                                                                                                                                                                                          |
| Step 7 | <b>show running-config</b><br><br><b>Example:</b><br>Router# show running-config                                                                                                      | Displays the running configuratoin of the router so that you can determine if an SNMP agent is already running on the device.<br><br>If you see any snmp-server statements, SNMP has been enabled on the router.<br><br>If any SNMP information is displayed, you can modify the information or change it as desired.                                                                                           |

# Configuration Examples for the MPLS Enhancements to Interfaces MIB

This section provides the following configuration examples:

- [MPLS Enhancements to Interfaces MIB: Examples, page 10](#)

## MPLS Enhancements to Interfaces MIB: Examples

The following example shows how to enable an SNMP agent:

```
Router# configure terminal  
Router(config)# snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro 4
```

## Additional References

The following sections provide references related to the MPLS Enhancements to Interfaces MIB feature.

## Related Documents

| Related Topic                                                                                                    | Document Title                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMP commands                                                                                                    | <ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Network Management Command Reference</a>, Release 12.4T</li> <li>• <a href="#">Cisco IOS Network Management Command Reference</a>, Release 12.2SB</li> <li>• <a href="#">Cisco IOS Network Management Command Reference</a>, Release 12.2SR</li> </ul>                                      |
| SNMP configuration                                                                                               | “Configuring SNMP support” in the <a href="#">Cisco IOS Network Management Configuration Guide</a> , Release 12.4                                                                                                                                                                                                                                          |
| A description of SNMP agent support in Cisco IOS software for the MPLS Label Switching Router MIB (MPLS-LSR-MIB) | <a href="#">MPLS Label Switching Router MIB</a>                                                                                                                                                                                                                                                                                                            |
| A description of SNMP agent support in Cisco IOS for the MPLS Traffic Engineering MIB (MPLS TE MIB)              | <a href="#">MPLS Traffic Engineering (TE) MIB</a>                                                                                                                                                                                                                                                                                                          |
| Other documentation                                                                                              | <p>“Multiprotocol Label Switching (MPLS) Label Switch Router (LSR) Management Information Base,” Internet draft, January 2002 [draft-ietf-mpls-lsr-mib-08.txt]; Srinivasan, C., Viswanathan, A., and Nadeau, T.D.</p> <p><b>Note</b> For information on using SNMP MIB features, see the appropriate documentation for your network management system.</p> |

## Standards

| Standards                                                                                                                             | Title |
|---------------------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature. | —     |

## MIBs

| MIBs                          | MIBs Link                                                                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interfaces Group MIB (IF MIB) | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFCs     | Title                                                                                       |
|----------|---------------------------------------------------------------------------------------------|
| RFC 1156 | <i>Management Information Base for Network Management of TCP/IP-based internets</i>         |
| RFC 1157 | <i>A Simple Network Management Protocol (SNMP)</i>                                          |
| RFC 1213 | <i>Management Information Base for Network Management of TCP/IP-based internets: MIB-II</i> |
| RFC 1229 | <i>Extensions to the Generic-Interface MIB</i>                                              |
| RFC 2233 | <i>Interfaces MIB</i>                                                                       |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, use the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **snmp-server community**

# Glossary

**ATM**—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

**ATM-AAL5**—ATM adaptation layer 5. One of four AALs recommended by the ITU-T. AAL5 supports connection-oriented variable bit rate (VBR) services and is used predominantly for the transfer of classical IP over ATM and LAN emulation (LANE) traffic. AAL5 uses simple and efficient AAL (SEAL) and is the least complex of the current AAL recommendations. It offers low bandwidth overhead and simpler processing requirements in exchange for reduced bandwidth capacity and error-recovery capability.

**encapsulation**—Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

**IETF**—Internet Engineering Task Force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

**interface**—The boundary between adjacent layers of the ISO model.

**label**—A short, fixed-length identifier that is used to determine the forwarding of a packet.

**label switching**—A term used to describe the forwarding of IP (or other network layer) packets using a label swapping algorithm based on network layer routing algorithms. The forwarding of these packets uses the exact match algorithm and rewrites the label.

**LSR**—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**MPLS interface**—An interface on which MPLS traffic is enabled.

**MTU**—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

**NMS**—network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

**OID**—object identifier. Values are defined in specific MIB modules. The Event MIB allows you or an NMS to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger is fired; this means that a specified test on an object returns a value of true. To create a trigger, you or an NMS configures a trigger entry in the `mteTriggerTable` of the Event MIB. This trigger entry specifies the OID of the object to be watched. For each trigger entry type, corresponding tables (existence, threshold, and Boolean tables) are populated with the information required for carrying out the test. The MIB can be configured so that when triggers are activated (fired) either an SNMP Set is performed, a notification is sent out to the interested host, or both.

**SNMP**—Simple Network Management Protocol. A management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**traffic engineering tunnel**—A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

**tunnel**—A secure communication path between two peers, such as routers.

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

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

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

© 2004–2008 Cisco Systems, Inc. All rights reserved.



# MPLS Label Switching Router MIB

The MPLS Label Switching Router MIB (MPLS-LSR-MIB) allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switch router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology.

Scalability enhancements provided in the Cisco IOS 12.0(28)S release reduce the size of any MIB walk and improve the usability of the MPLS-LSR-MIB.

ort the Internet Engineering Task Force (IETF) draft Version 8.



**Note** In Cisco IOS Release 12.2(33)SRB and Cisco IOS Release 12.2(33)SB, this MIB has been deprecated and replaced by MPLS-LSR-STD-MIB (RFC 3813). In those two releases and in later images, the entire MIB can be referenced by the name `mplsLsrMIB` for purposes of the SNMP `server excluded/included` command. If other MIB object names need to be referenced on the router, they must be referenced by `MPLS-LSR-MIB::<table_entry_name>`.

## Feature History for MPLS Label Switching Router MIB

| Release     | Modification                                                                                                              |
|-------------|---------------------------------------------------------------------------------------------------------------------------|
| 12.0(14)ST  | This feature was introduced on Cisco IOS Release 12.0(14)ST                                                               |
| 12.2(2)T    | This feature was integrated into Cisco IOS Release 12.2(2)T.                                                              |
| 12.0(22)S   | This feature was implemented on the Cisco 12000 series routers and integrated into Cisco IOS Release 12.0(22)S.           |
| 12.2(14)S   | This feature was integrated into Cisco IOS Release 12.2(14)S and implemented on Cisco 7200 and Cisco 7500 series routers. |
| 12.2(25)S   | This feature was updated to work in the MPLS High Availability environment with the Cisco 7500 series routers.            |
| 12.0(28)S   | This feature was updated to include scalability enhancements in Cisco IOS Release 12.0(28)S.                              |
| 12.2(33)SRB | This MIB has been deprecated and replaced by MPLS-LSR-STD-MIB (RFC 3813).                                                 |
| 12.2(33)SB  | This MIB has been deprecated and replaced by MPLS-LSR-STD-MIB (RFC 3813).                                                 |



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

© 2007 Cisco Systems, Inc. All rights reserved.



### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

## Contents

This document includes the following major sections:

- [Information About MPLS Label Switching Router MIB, page 2](#)
- [How to Configure the MPLS LSR MIB, page 13](#)
- [Configuration Examples for the MPLS LSR MIB, page 15](#)
- [Additional References, page 16](#)
- [Command Reference, page 17](#)
- [Glossary, page 17](#)

## Information About MPLS Label Switching Router MIB

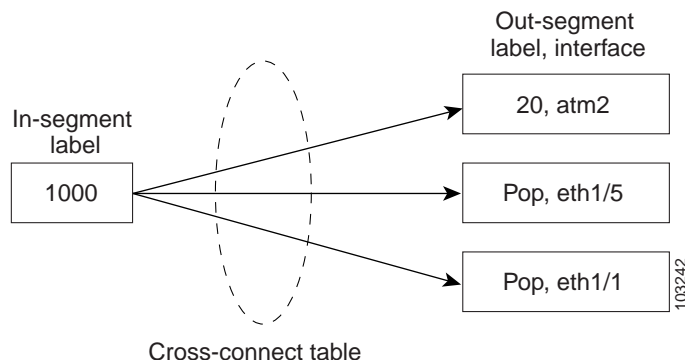
The MPLS-LSR-MIB contains managed objects that support the retrieval of label switching information from a router. The MIB is based on Revision 05 of the IETF MPLS-LSR-MIB. The MPLS-LSR-MIB mirrors a portion of the Cisco MPLS subsystem; specifically, it mirrors the Label Forwarding Information Base (LFIB). This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS-capable interfaces on the LSR
- Incoming MPLS segments (labels) at an LSR and their associated parameters
- Outgoing segments (labels) at an LSR and their associated parameters

In addition, the network administrator can retrieve the status of cross-connect table entries that associate MPLS segments with each other.

[Figure 1](#) shows the association of the cross-connect table with incoming and outgoing segments (labels).

**Figure 1** *Label Forwarding with the Cross-Connect Table*



**Note**

The out-segment table does not display “no label” entries. Labels that are displayed as “POP” are the special MPLS label 3.

The notation used in the MPLS-LSR-MIB follows the conventions defined in Abstract System Notation One (ASN.1). ASN.1 defines an Open System Interconnection (OSI) language used to describe data types apart from particular computer structures and presentation techniques. Each object in the MIB incorporates a DESCRIPTION field that includes an explanation of the object’s meaning and usage, which, together with the other characteristics of the object (SYNTAX, MAX-ACCESS, and INDEX) provides sufficient information for management application development, as well as for documentation and testing.

The MPLS-LSR-MIB represents an ASN.1 notation reflecting an idealized MPLS LSR.

A network administrator can access the entries (objects) in the MPLS-LSR-MIB by means of any SNMP-based network management system (NMS). The network administrator can retrieve information in the MPLS-LSR-MIB using standard SNMP **get** and **getnext** operations.

Typically, SNMP runs as a low-priority process. The response time for the MPLS-LSR-MIB is expected to be similar to that for other MIBs. The size and structure of the MIB and other MIBs in the system influence response time when you retrieve information from the management database. Traffic through the LSR also affects SNMP performance. The busier the switch is with forwarding activities, the greater the possibility of lower SNMP performance.

## MPLS-LSR-MIB Elements

The top-level components of the MPLS-LSR-MIB consist of

- Tables and scalars (mplsLsrObjects)
- Traps (mplsLsrNotifications and mplsLsrNotifyPrefix)
- Conformance (mplsLsrConformance)

This Cisco implementation does not support the notifications defined in the MIB, nor does it support the labelStackTable or the trafficParamTable.

## MPLS-LSR-MIB Tables

The Cisco implementation of the MPLS-LSR-MIB supports four main tables:

- Interface configuration
- In-segment
- Out-segment
- Cross-connect

The MIB contains three supplementary tables to supply performance information. This implementation does not support the label stack and traffic parameter tables.

The following sections list the MPLS-LSR-MIB tables (main and supplementary), their functions, table objects that are supported, and table objects that are *not* supported.

### **MPLS interface configuration table (mplsInterfaceConfTable)**

Provides information for each MPLS-capable interface on an LSR.

Supports:

- A unique interface index or zero
- Minimum and maximum values for an MPLS label received on the interface
- Minimum and maximum values for an MPLS label sent from the interface
- A value for an MPLS label sent from the interface
- Per platform (0) or per interface (1) setting
- The storage type

Does not support:

- The total usable bandwidth on the interface
- The difference between the total usable bandwidth and the bandwidth in use

#### **MPLS interface performance table (mplsInterfacePerfTable)**

Augments the MPLS interface configuration table.

Supports:

- The number of labels in the incoming direction in use
- The number of top-most labels in outgoing label stacks in use

Does not support:

- The number of top-most labels in outgoing label stacks in use
- The number of labeled packets discarded because no cross-connect entries exist
- The number of outgoing MPLS packets requiring fragmentation for transmission

#### **MPLS in-segment table (mplsInSegmentTable)**

Contains a description of incoming segments (labels) at an LSR and their associated parameters.

Administrative and operational status objects for this table control packet transmission. If administrative and operational status objects are down, the LSR does not forward packets. If these status objects are up, the LSR forwards packets.

Supports:

- A unique index identifier
- The incoming label
- The number of labels to pop from the incoming segment
- An address family number from the Internet Assigned Number Authority (IANA)
- A segment cross-connect entry association
- The segment owner
- The storage type
- The administrative status
- The operational status



#### **Note**

The administrative status and operational status are always up for inSegments in the Cisco implementation. Otherwise, these entries do not appear in the table.

Does not support:

- A pointer to a traffic parameter table entry (set to the default 0.0)

#### **MPLS in-segment performance table (mplsInSegmentPerfTable)**

Augments the MPLS in-segment table, providing performance information and counters for incoming segments on an LSR.

Supports:

- The number of 32-bit octets received
- The number of 64-bit octets received
- The time of the last system failure that corresponded to one or more incoming segment discontinuities



#### **Note**

---

The lastFailure parameter is set to zero because it has no meaning in the Cisco implementation.

---

Does not support:

- The total number of packets received
- The number of packets with errors
- The number of labeled packets discarded with no errors

#### **MPLS out-segment table (mplsOutSegmentTable)**

Contains a description of outgoing segments from an LSR and their associated parameters.

Administrative and operational status objects for this table control packet transmission. If administrative and operational status objects are down, the LSR does not forward packets. If these values are up, the LSR forwards packets.

Supports:

- A unique index identifier
- An interface index of the outgoing interface
- An indication of whether or not a top label is pushed onto the outgoing packet's label stack
- The label to push onto the outgoing packet's label stack (if the previous value is true)
- The next hop address type
- The IPv4 address of the next hop
- The segment cross-connect entry association
- The segment owner
- The storage type
- The administrative status
- The operational status



#### **Note**

---

The administrative and operational status entries are always up in the Cisco implementation. Otherwise, the administrative and operational status entries do not appear in the table.

---

Does not support:

- An IPv6 address of the next hop
- A pointer to a traffic parameter table entry (set to the default 0.0)

#### **MPLS out-segment performance table (mplsOutSegmentPerfTable)**

Augments the MPLS out-segment table, providing performance information and counters for outgoing segments on an LSR.

Supports:

- The number of 32-bit octets sent
- The number of 64-bit octets sent
- The time of the last system failure that corresponded to one or more outgoing segment discontinuities

Does not support:

- The number of packets sent
- The number of packets that could not be sent because of errors
- The number of packets discarded with no errors

#### **MPLS cross-connect table (mplsXCTable)**

Associates inSegments (labels) with outSegments (labels) to show the manager how the LSR is currently swapping these labels.

A row in this table consists of one cross-connect entry that is indexed by the cross-connect index, the interface index of the incoming segment, the incoming label, and the out-segment index.

The administrative and operational objects for this table control packet forwarding to and from a cross-connect entry (XCEntry). The administrative status and operational status are always up in the Cisco implementation. Otherwise, the LSR would not forward packets.

Supports:

- A unique index identifier for a group of cross-connect segments
- A label switched path (LSP) to which the cross-connect entry belongs
- An index to the MPLS label stack table that identifies the stack of labels to be pushed under the top label
- An indication whether or not to restore the cross-connect entry after a failure (the default value is false)
- The cross-connect owner
- The storage type
- The administrative status (if up)
- The operational status (if up)



#### **Note**

The administrative status and operational status are always up in the Cisco implementation. Otherwise, these status entries do not appear in the table.

Does not support:

- Tunnel IDs as label switched path (LSP) ID objects

## Information from Scalar Objects

The MPLS-LSR-MIB supports several scalar objects. In the Cisco implementation of the MIB, the following scalar objects are hard-coded to the value indicated and are read-only objects:

- `mplsOutSegmentIndexNext (0)`—The value for the out-segment index when an LSR creates a new entry in the MPLS out-segment table. The 0 indicates that this is not implemented because modifications to this table are not allowed.
- `mplsXCTIndexNext (0)`—The value for the cross-connect index when an LSR creates an entry in the MPLS cross-connect table. The 0 indicates that no unassigned values are available.
- `mplsMaxLabelDepth(2)`—The value for the maximum stack depth.
- `mplsLabelStackIndexNext (0)`—The value for the label stack index when an LSR creates entries in the MPLS label stack table. The 0 indicates that no unassigned values are available.
- `mplsTrafficParamIndexNext (0)`—The value for the traffic parameter index when an LSR creates entries in the MPLS traffic parameter table. The 0 indicates that no unassigned values are available.

The following scalar objects do not contain information for the MPLS-LSR-MIB and are coded as false:

- `mplsInSegmentTrapEnable (false)`—In-segment traps are not sent when this value is false.
- `mplsOutSegmentTrapEnable (false)`—Out-segment traps are not sent when this value is false.
- `mplsXCTrapEnable (false)`—Cross-connect traps are not sent when this value is false.

No trap information exists to support the MIB. Therefore, the following traps are not supported:

- `mplsInSegmentUp`
- `mplsInSegmentDown`
- `mplsOutSegmentUp`
- `mplsOutSegmentDown`
- `mplsXCUp`
- `mplsXCDown`

## Linking Table Elements

In the cross-connect table, cross-connect entries associate incoming segments and interfaces with outgoing segments and interfaces. The following objects index the cross-connect entry:

- **Cross-connect index**—A unique identifier for a group of cross-connect entries in the cross-connect table. In the Cisco implementation, this value is always the same as that for the `outSegmentIndex`, unless there is no label or if the label has been popped.
- **Interface index of the in-segment**—A unique index for an entry in the in-segment table that represents an incoming MPLS interface. The value 0 means platform wide, for any entries that apply to all interfaces.
- **Incoming label**—An entry in the in-segment table that represents the label on the incoming packet.
- **Out-segment index**—A unique identifier for an entry in the out-segment table that contains a top label for the outgoing packet's label stack and an interface index of the outgoing interface.

Figure 2 shows the links between the in-segment and the out-segment in the cross-connect table.

**Figure 2** *Cross-Connect Table Links*

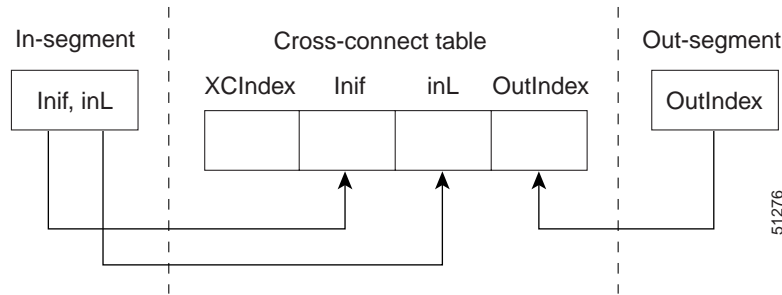


Table 1 shows the cross-connect table links you might see in the output from SNMP **get** operations on the MPLS-LSR-MIB objects that index a cross-connect entry. These objects include

- In-Segment Values—mplsInSegmentIfIndex and mplsInSegmentLabel
- Cross-Connect Entry—mplsXCIndex
- Out-Segment Values—mplsOutSegmentIndex

**Table 1** *MPLS LSR Output Showing Cross-Connect Table Links*

| In-Segment Values     | Cross-Connect Entry                        | Out-Segment Values              |
|-----------------------|--------------------------------------------|---------------------------------|
| 0 <sup>1</sup> , 1000 | 500 <sup>2</sup> , 0, 1000, 0 <sup>2</sup> | —                               |
|                       | 501, 0, 1000, 501                          | 501 = Pop (topLabel), Eth 1/5   |
|                       | 502, 0, 1000, 502                          | 502 = Pop (topLabel), Eth, 1/1) |

1. All MPLS-enabled interfaces can receive incoming labels.
2. For this implementation of the MPLS-LSR-MIB, the cross-connect index and the out-segment index are the same. If there is no outsegment, the value will be zero.



**Note**

The OutSegmentIndex object is not the label. The label can be retrieved from the mplsOutSegmentTopLabel object.

## Interface Configuration Table and Interface MIB Links

The MPLS interface configuration table lists interfaces that support MPLS technology. An LSR creates an entry dynamically in this table for each MPLS-capable interface. An interface becomes MPLS-capable when MPLS is enabled on that interface. A non-zero index for an entry in this table points to the ifIndex for the corresponding interface entry in the ifTable of the Interfaces Group MIB.

The ifTable contains information on each interface in the network. Its definition of an interface includes any sublayers of the internetwork layer of the interface. MPLS interfaces fit into this definition of an interface. Therefore, each MPLS-enabled interface is represented by an entry in the ifTable.

The interrelation of entries in the ifTable is defined by the interfaces stack group of the Interfaces Group MIB. Figure 3 shows how the stack table might appear for MPLS interfaces. The underlying layer refers to any interface that is defined for MPLS internetworking, for example, ATM, Frame Relay, or Ethernet.

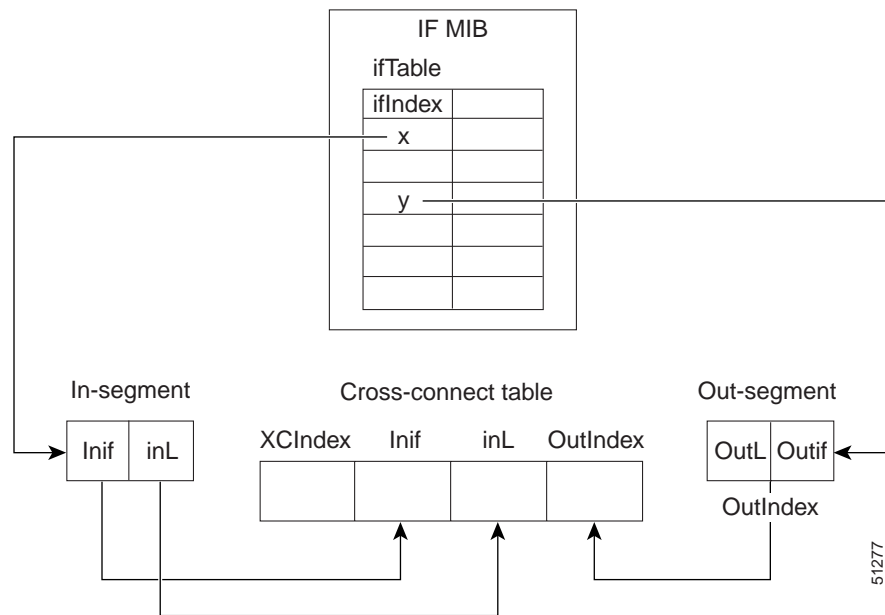
**Figure 3** *Interface Group MIB Stack Table for MPLS Interfaces*

|                                   |       |
|-----------------------------------|-------|
| MPLS-interface ifType = mpls(166) | 51273 |
| Underlying Layer . . .            |       |

**Note**

Tunnel interfaces are included in the MPLS list for the current implementation.

The incoming and outgoing packets include a reference to the interface index for the ifTable of the Interfaces Group MIB. [Figure 4](#) shows the links between MPLS-LSR-MIB objects and the Interfaces Group MIB.

**Figure 4** *MPLS-LSR-MIB and Interfaces Group MIB Links*

- For the Interfaces Group MIB (IF MIB):
  - ifTable represents the MPLS interface table.
  - ifIndex represents the index to an entry in the MPLS interface table.
- For the In-segment:
  - Inif represents the interface on the incoming segment (references an index entry in the ifTable).
  - inL represents the label on the incoming segment.
- For the Out-segment:
  - OutL represents the label on the outgoing segment.
  - Outif represents the interface on the outgoing segment (references an index entry in the ifTable).
- For the Cross-connect table:
  - XCIndex represents the index to an entry in the MPLS cross-connect table.



- Inif represents the interface on the incoming segment.
- inL represents the MPLS label on the incoming segment.
- OutIndex represents an index to an entry in the MPLS out-segment table.

## Using the MPLS-LSR-MIB

The MPLS-LSR-MIB enables you to display the contents of the MPLS Label Forwarding Information Base (LFIB). It gives you the same information that you can obtain using the CLI command **show mpls forwarding-table**.

However, the MPLS-LSR-MIB approach offers these advantages over the CLI command approach:

- A more efficient use of network bandwidth
- Greater interoperability among vendors
- Greater security (SMNP Version 3)

The following paragraphs describe the MPLS-LSR-MIB structure and show, through the use of an example, how the two approaches to the information display compare.

### MPLS-LSR-MIB Structure

MIB structure is represented by a tree hierarchy. Branches along the tree have short text strings and integers to identify them. Text strings describe object names, and integers allow computer software to encode compact representations of the names.

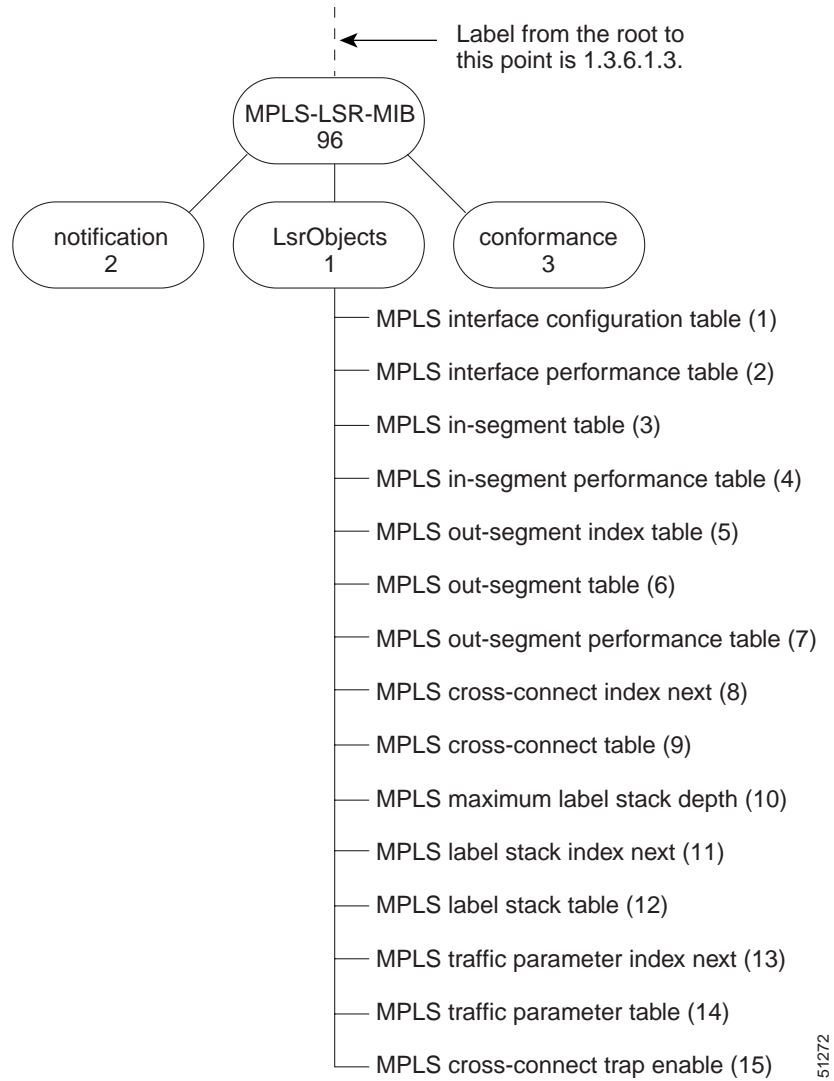
The MPLS-LSR-MIB falls on the experimental branch of the Internet MIB hierarchy. The experimental branch of the Internet MIB hierarchy is represented by the object identifier 1.3.6.1.3. This branch can also be represented by its object name *iso.org.dod.internet.experimental*. The MPLS-LSR-MIB is identified by the object name *mplsLsrMIB*, which is denoted by the number 96. Therefore, objects in the MPLS-LSR-MIB can be identified in either of the following ways:

- The object identifier—1.3.6.1.3.96.[MIB-variable]
- The object name—*iso.org.dod.internet.experimental.mplsLsrMIB.[MIB-variable]*

To display a *MIB-variable*, you enter an SNMP **get** command with an object identifier. Object identifiers are defined by the MPLS-LSR-MIB.

Figure 5 shows the position of the MPLS-LSR-MIB in the Internet MIB hierarchy.

**Figure 5** *MPLS-LSR-MIB in the Internet MIB Hierarchy*



## CLI Commands and the MPLS-LSR-MIB

The MPLS LFIB is the component of the Cisco MPLS subsystem that contains management information for LSRs. You can access this management information by means of either of the following:

- Using the **show mpls forwarding-table** CLI command
- Entering SNMP **get** commands on a network manager

The following examples show how you can gather LSR management information using both methods.

### CLI Command Output

A **show mpls forwarding-table** CLI command allows you to look at label forwarding information for a packet on a specific MPLS LSR.

Router# **show mpls forwarding-table**

| Local Tag | Outgoing Tag or VC | Prefix or Tunnel Id | Bytes Tag Switched | Outgoing interface | Next Hop    |
|-----------|--------------------|---------------------|--------------------|--------------------|-------------|
| 19        | Pop Tag            | 10.3.4.0/24         | 0                  | Et1/4              | 10.22.23.23 |
| 22        | 23                 | 14.14.14.14/32      | 0                  | AT2/0.1            | point2point |
|           | 1/36               | 14.14.14.14/32      | 0                  | AT2/0.2            | point2point |

### MPLS-LSR-MIB Output

SNMP commands on MIB objects also allow you to look at the label forwarding information for a specific MPLS LSR.

You can do a walk-through of the MIB by running a command such as **getmany -v2c public mplsLsrMIB** on a network manager where **getmany** does repeated SNMP **getnext** operations to retrieve the contents of the MPLS-LSR-MIB.

```
mplsXCOperStatus.9729.0.19.9729 = up(1)
mplsXCOperStatus.11265.0.22.11265 = up(1)
mplsXCOperStatus.11266.0.22.11266 = up(1)
```

You can continue to scan the output of the **getmany** command for the following (from the MPLS out-segment table):

- Out-segment's top label objects (mplsOutSegmentTopLabel)

```
mplsOutSegmentTopLabel.9729 = 3
mplsOutSegmentTopLabel.11265 = 23
mplsOutSegmentTopLabel.11266 = 65572
```



#### Note

65572 is 1/36 in label form (1 is the high-order 16 bits. 36 is the low-order 16 bits.)

- Out-segment's interface index (mplsOutSegmentIfIndex)

```
mplsOutSegmentIfIndex.9729 = 7
mplsOutSegmentIfIndex.11265 = 28
mplsOutSegmentIfIndex.11266 = 31
```

## Benefits

The benefits described in the following paragraphs are available to you with the MPLS-LSR-MIB.

### Troubleshooting LSR Problems

By monitoring the cross-connect entries and the associated incoming and outgoing segments, you can see which labels are installed and how they are being swapped. Use the MPLS-LSR-MIB in place of the **show mpls forwarding** CLI command.

### Monitoring of LSR Traffic Loads

By monitoring interface and packet operations on an MPLS LSR, you can identify high- and low-traffic patterns, as well as traffic distributions.

### Improvement of Network Performance

By identifying potentially high-traffic areas, you can set up load sharing to improve network performance.

### Verification of LSR Configuration

By comparing results from SNMP **get** commands and the **show mpls forwarding** CLI command, you can verify your LSR configuration.

### Displaying of Active Label Switched Paths

By monitoring the cross-connect entries and the associated incoming segments and outgoing segments, you can determine the active LSPs.

## How to Configure the MPLS LSR MIB

See the following sections for configuration tasks for the MPLS-LSR-MIB feature. Each task in the list is identified as either optional or required.

- [Enabling the SNMP Agent](#) (required)
- [Verifying That the SNMP Agent Has Been Enabled](#) (optional)

## Prerequisites

The MPLS-LSR-MIB requires the following:

- SNMP installed and enabled on the LSR
- MPLS enabled on the LSR
- 60K of memory



---

**Note** Additional capacity is not required for runtime dynamic random-access memory (DRAM).

---

## Enabling the SNMP Agent

The SNMP agent for the MPLS-LSR-MIB is disabled by default. To enable the SNMP agent, perform the following steps:

### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro**] [*number*]
5. **end**
6. **copy running-config startup-config**

### DETAILED STEPS

|        | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                        |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                                                                                                                | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                             |
| Step 2 | <b>show running-config</b><br><br><b>Example:</b><br>Router# show running-config                                                                                                      | Displays the running configuration of the router to determine if an SNMP agent is already running on the device.<br><br>If no SNMP information is displayed, continue with the next step.<br><br>If any SNMP information is displayed, you can modify the information or change it as desired. |
| Step 3 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal                                                                                                        | Enters global configuration mode.                                                                                                                                                                                                                                                              |
| Step 4 | <b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b> ] [ <i>number</i> ]<br><br><b>Example:</b><br>Router(config)# snmp-server community public ro | Configures read-only (ro) SNMP community strings.<br><br>This command enables the SNMP agent and permits any SNMP manager to access all objects with read-only permission using the community string public.                                                                                   |

|        | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                  |
|--------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 5 | <code>end</code><br><br><b>Example:</b><br><code>Router(config)# end</code>                                                       | Exits to privileged EXEC mode.                                                                                                                                                                           |
| Step 6 | <code>copy running-config startup-config</code><br><br><b>Example:</b><br><code>Router# copy running-config startup-config</code> | Copies the modified SNMP configuration into router NVRAM, permanently saving the SNMP settings.<br><br>When you are working with Cisco IOS Release 10.3 or earlier, use the <b>write memory</b> command. |

## Verifying That the SNMP Agent Has Been Enabled

To verify that the SNMP agent has been enabled, perform the following steps:

- 
- Step 1** Access the router through a Telnet session:
- ```
Prompt# telnet xxx.xxx.xxx.xxx
```
- where `xxx.xxx.xxx.xxx` represents the IP address of the target device.
- Step 2** Enter privileged mode:
- ```
Router# enable
```
- Step 3** Display the running configuration and look for SNMP information:
- ```
Router# show running-configuration
...
...
snmp-server community public RO
```
- If you see any “snmp-server” statements, SNMP has been enabled on the router.
- 

## Configuration Examples for the MPLS LSR MIB

The following example shows how to enable an SNMP agent.

```
configure terminal
snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
configure terminal
snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the *comaccess* community string. No other SNMP managers have access to any objects.

```
configure terminal
snmp-server community comaccess ro 4
```

# Additional References

The following sections provide references related to the MPLS LSR MIB.

## Related Documents

Related Topic	Document Title
Configuring SNMP using Cisco IOS software	<ul style="list-style-type: none"> <li>• <a href="#">Cisco IOS Network Management Configuration Guide, Release 12.4</a>, Configuring SNMP Support</li> <li>• <a href="#">Cisco IOS Network Management Command Reference, Release 12.4</a>, SNMP Commands</li> </ul>

## Standards

Standard	Title
draft-ietf-mpls-lsr-mib-05.txt	MPLS Label Switch Router Management Information Base Using SMIv2
draft-ietf-mpls-arch-07.txt	Multiprocol Label Switching Architecture

## MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> <li>• MPLS Label Switching Router MIB (MPLS-LSR-MIB)</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFCs	Title
The LSR implementation supporting the MPLS-LSR-MIB is in full compliance with all provisions of Section 10 of RFC 2026.	<i>The Internet Standards Process</i>

## Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This feature uses no new or modified commands.

## Glossary

**cross-connect (XC)**—An association of in-segments and incoming Multiprotocol Label Switching (MPLS) interfaces to out-segments and outgoing MPLS interfaces.

**IETF**—Internet Engineering Task Force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

**inSegment**—A label on an incoming packet that is used to determine the forwarding of the packet.

**Internet Engineering Task Force**—See IETF.

**label**—A short, fixed length identifier that is used to determine the forwarding of a packet.

**Label Distribution Protocol**—See LDP.

**label switched path**—See LSP.

**label switching**—Describes the forwarding of IP (or other network layer) packets by a label swapping algorithm based on network layer routing algorithms. The forwarding of these packets uses the exact match algorithm and rewrites the label.

**label switch router**—See LSR.

**LDP**—Label Distribution Protocol. A standard protocol that operates between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label switched path. A sequence of hops in which a packet travels from one router to another router by means of label switching mechanisms. A label switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

**LSR**—label switch router. A device that forwards Multiprotocol Label Switching (MPLS) packets based on the value of a fixed-length label encapsulated in each packet.

**Management Information Base**—See MIB.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.



**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic through use of a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

**MPLS interface**—An interface on which Multiprotocol Label Switching (MPLS) traffic is enabled.

**Multiprotocol Label Switching**—See MPLS.

**notification request**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal, indicating that a significant event occurred. SNMP notification requests are more reliable than traps, because a notification request from an SNMP agent requires that the SNMP manager acknowledge receipt of the notification request. The manager replies with an SNMP response protocol data unit (PDU). If the manager does not receive a notification message from an SNMP agent, it does not send a response. If the sender (SNMP agent) never receives a response, the notification request can be sent again.

**outSegment**—A label on an outgoing packet.

**Simple Network Management Protocol**—See SNMP.

**SNMP**—Simple Network Management Protocol. A management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**trap**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

**Note**

Refer to the Cisco [Dictionary of Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS Label Distribution Protocol MIB Version 8 Upgrade

**First Published: November 13, 2000**

**Last Updated: March 06, 2009**

The MPLS Label Distribution Protocol (LDP) MIB Version 8 Upgrade feature enhances the LDP MIB to support the Internet Engineering Task Force (IETF) draft Version 8.



**Note**

In Cisco IOS Release 12.2(33)SRB and Cisco IOS Release 12.2(33)SB, this MIB has been deprecated and replaced by MPLS-LDP-STD-MIB (RFC 3815). In those two releases and in later images, the entire MIB can be referenced by the name `mplsLdpMIB` for purposes of the `SNMP server excluded/included` command. If other MIB object names need to be referenced on the router, they must be referenced by `MPLS-LDP-MIB::<table_entry_name>`.

## History for MLPS Label Distribution Protocol MIB Version 8 Update Feature

Release	Modification
12.0(11)ST	This feature was introduced to provide SNMP agent support for the MPLS LDP MIB on Cisco 7200, Cisco 7500, and Cisco 12000 series routers.
12.2(2)T	This feature was added to this release to provide SNMP agent support for the MPLS LDP MIB on Cisco 7200 and Cisco 7500 series routers.
12.0(21)ST	This feature was added to this release to provide SNMP agent and LDP notification support for the MPLS LDP MIB on Cisco 7200, Cisco 7500, and Cisco 12000 series Internet routers.
12.0(22)S	This feature (Version 1) was integrated into Cisco IOS Release 12.0(22)S.
12.0(24)S	This feature was upgraded to Version 8 in Cisco IOS Release 12.0(24)S.
12.0(27)S	Support for the MPLS VPN—VPN Aware LDP MIB feature was added.
12.2(18)S	This feature was integrated into Cisco IOS Release 12.2(18)S.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.



**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

12.2(33)SRB	This MIB has been deprecated and replaced by MPLS-LDP-STD-MIB (RVC 3815).
12.2(33)SB	This MIB has been deprecated and replaced by MPLS-LDP-STD-MIB (RVC 3815).

### Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS LDP MIB Version 8 Upgrade, page 2](#)
- [Restrictions for MPLS LDP MIB Version 8 Upgrade, page 2](#)
- [Information About MPLS LDP MIB Version 8 Upgrade, page 3](#)
- [Description of MPLS LDP MIB Elements for MPLS LDP MIB Version 8 Upgrade, page 6](#)
- [Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade, page 9](#)
- [MIB Tables in MPLS LDP MIB Version 8 Upgrade, page 11](#)
- [VPN Contexts in MPLS LDP MIB Version 8 Upgrade, page 20](#)
- [How to Configure MPLS LDP MIB Version 8 Upgrade, page 25](#)
- [Configuration Examples for MPLS LDP MIB Version 8 Upgrade, page 37](#)
- [Additional References, page 39](#)
- [Command Reference, page 41](#)
- [Glossary, page 42](#)

## Prerequisites for MPLS LDP MIB Version 8 Upgrade

- Simple Network Management Protocol (SNMP) must be installed and enabled on the label switch routers (LSRs).
- Multiprotocol Label Switching (MPLS) must be enabled on the LSRs.
- LDP must be enabled on the LSRs.

## Restrictions for MPLS LDP MIB Version 8 Upgrade

This implementation of the MPLS LDP MIB is limited to read-only (RO) permission for MIB objects, except for MIB object *mplsLdpSessionUpDownTrapEnable*, which has been extended to be writable by the SNMP agent.

Setting this object to a value of true enables both the *mplsLdpSessionUp* and *mplsLdpSessionDown* notifications on the LSR; conversely, setting this object to a value of false disables both of these notifications.

For a description of notification events, see the [“Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade”](#) section on page 9.

Most MPLS LDP MIB objects are set up automatically during the LDP peer discovery (hello) process and the subsequent negotiation of parameters and establishment of LDP sessions between the LDP peers.

The following tables are not implemented in this feature:

- `mplsLdpEntityFrParmsTable`
- `mplsLdpEntityConfFrLRTable`
- `mplsLdpFrameRelaySesTable`
- `mplsFecTable`
- `mplsLdpSesInLabelMapTable`
- `mplsXCsfecsTable`
- `mplsLdpSesPeerAddrTable`

## Information About MPLS LDP MIB Version 8 Upgrade

To configure MPLS LDP MIB Version 8 Upgrade, you need to understand the following concepts:

- [Feature Design of MPLS LDP MIB Version 8 Upgrade, page 3](#)
- [Enhancements in Version 8 of the MPLS LDP MIB, page 5](#)
- [Benefits of MPLS LDP MIB Version 8 Upgrade, page 5](#)

## Feature Design of MPLS LDP MIB Version 8 Upgrade

MPLS is a packet forwarding technology that uses a short, fixed-length value called a label in packets to specify the next hop for packet transport through an MPLS network by means of label switch routers (LSRs).

A fundamental MPLS principle is that LSRs in an MPLS network must agree on the definition of the labels being used for packet forwarding operations. Label agreement is achieved in an MPLS network by means of procedures defined in the LDP.

LDP operations begin with a discovery (hello) process, during which an LDP entity (a local LSR) finds a cooperating LDP peer in the network, and the two negotiate basic operating procedures. The recognition and identification of a peer by means of this discovery process results in a hello adjacency, which represents the context within which label binding information is exchanged between the local LSR and its LDP peer. LDP then creates an active LDP session between the two LSRs to effect the exchange of label binding information. When this process is carried to completion with respect to all of the LSRs in an MPLS network, the result is a label-switched path (LSP), which constitutes an end-to-end packet transmission pathway between the communicating network devices.

By means of LDP, LSRs can collect, distribute, and release label binding information to other LSRs in an MPLS network, thereby enabling the hop-by-hop forwarding of packets in the network along normally routed paths.

The MPLS LDP MIB has been implemented to enable standard, SNMP-based network management of the label switching features in Cisco IOS software. Providing this capability requires SNMP agent code to execute on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MPLS LDP MIB.

The SNMP agent code has a layered structure that is compatible with Cisco IOS software and presents a network administrative and management interface to the objects in the MPLS LDP MIB and, thence, to the rich set of label switching capabilities supported by Cisco IOS software.

By means of an SNMP agent, you can access MPLS LDP MIB objects using standard SNMP GET operations, and you can use those objects to accomplish a variety of network management tasks. All the objects in the MPLS LDP MIB follow the conventions defined in the IETF draft MIB entitled *draft-ietf-mpls-ldp-mib-08.txt*, which defines network management objects in a structured and standardized manner. This draft MIB is evolving and is soon expected to be a standard. Accordingly, the MPLS LDP MIB will be implemented in such a way that it tracks the evolution of this IETF document.

However, slight differences exist between the IETF draft MIB and the implementation of equivalent Cisco IOS functions. As a result, some minor translations between the MPLS LDP MIB objects and the internal Cisco IOS data structures are needed. Such translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low-priority process.

The extensive Cisco IOS label switching capabilities provide an integrated approach to managing the large volumes of traffic carried by WANs. These capabilities are integrated into the Layer 3 network services, thus optimizing the routing of high-volume traffic through Internet service provider backbones while, at the same time, ensuring the resistance of the network to link or node failures.

Cisco IOS Release 12.0(11)ST and later releases support the following MPLS LDP MIB-related functions:

- Tag Distribution Protocol (TDP)
- Generation and sending of event notification messages that signal changes in the status of LDP sessions
- Enabling and disabling of event notification messages by means of extensions to existing SNMP CLI commands
- Specification of the name or the IP address of an NMS workstation in the operating environment to which Cisco IOS event notification messages are to be sent to serve network administrative and management purposes
- Storage of the configuration pertaining to an event notification message in NVRAM of the NMS

The structure of the MPLS LDP MIB conforms to Abstract Syntax Notation One (ASN.1), so the MIB forms a highly structured and idealized database of network management objects.

Using any standard SNMP application, you can retrieve and display information from the MPLS LDP MIB by means of standard SNMP GET and GETNEXT operations.



#### Note

Because the MPLS LDP MIB was not given an Internet Assigned Numbers Authority (IANA) experimental object identifier (OID) at the time of its implementation, Cisco chose to implement the MIB under the `ciscoExperimental` OID number, as follows:

```
ciscoExperimental
1.3.6.1.4.1.9.10
mplsLdpMIB
1.3.6.1.4.1.9.10.65
```

If the MPLS LDP MIB is assigned an IANA Experimental OID number, Cisco will replace all objects in the MIB under the `ciscoExperimental` OID and reposition the objects under the IANA Experimental OID.

## Enhancements in Version 8 of the MPLS LDP MIB

Version 8 of the MPLS LDP MIB contains the following enhancements:

- TDP support
- Upgraded objects
- New indexing that is no longer based on the number of sessions
- Multiple SNMP context support for Virtual Private Networks (VPNs)

## Benefits of MPLS LDP MIB Version 8 Upgrade

- Supports TDP and LDP
- Establishes LDP sessions between peer devices in an MPLS network
- Retrieves MIB parameters relating to the operation of LDP entities, such as:
  - Well-known LDP discovery port
  - Maximum transmission unit (MTU)
  - Proposed keepalive timer interval
  - Loop detection
  - Session establishment thresholds
  - Range of virtual path identifier/virtual channel identifier (VPI/VCI) pairs to be used in forming labels
- Gathers statistics related to LDP operations, such as error counters ([Table 5](#))
- Monitors the time remaining for hello adjacencies
- Monitors the characteristics and status of LDP peers, such as:
  - Internetwork layer address of LDP peers
  - Loop detection of the LDP peers
  - Default MTU of the LDP peer
  - Number of seconds the LDP peer proposes as the value of the keepalive interval
- Monitors the characteristics and status of LDP sessions, such as:
  - Displaying the error counters ([Table 10](#))
  - Determining the LDP version being used by the LDP session
  - Determining the keepalive hold time remaining for an LDP session
  - Determining the state of an LDP session (whether the session is active or not)
  - Displaying the label ranges ([Table 2](#)) for platform-wide and interface-specific sessions
  - Displaying the ATM parameters ([Table 3](#))

# Description of MPLS LDP MIB Elements for MPLS LDP MIB Version 8 Upgrade

LDP operations related to an MPLS LDP MIB involve the following functional elements:

- LDP entity—Relates to an instance of LDP for purposes of exchanging label spaces; describes a potential session.
- LDP peer—Refers to a remote LDP entity (that is, a nonlocal LSR).
- LDP session—Refers to an active LDP process between a local LSR and a remote LDP peer.
- Hello adjacency—Refers to the result of an LDP discovery process that affirms the state of two LSRs in an MPLS network as being adjacent to each other (that is, as being LDP peers). When the neighbor is discovered, the neighbor becomes a hello adjacency. An LDP session can be established with the hello adjacency. After the session is established, label bindings can be exchanged between the LSRs.

These MPLS LDP MIB elements are briefly described under separate headings below.

In effect, the MPLS LDP MIB provides a network management database that supports real-time access to the various MIB objects in the database. This database reflects the current state of MPLS LDP operations in the network. You can access this network management information database by means of standard SNMP commands issued from an NMS in the MPLS LDP operating environment.

The MPLS LDP MIB supports the following network management and administrative activities:

- Retrieving MPLS LDP MIB parameters pertaining to LDP operations
- Monitoring the characteristics and the status of LDP peers
- Monitoring the status of LDP sessions between LDP peers
- Monitoring hello adjacencies in the network
- Gathering statistics regarding LDP sessions

## LDP Entities

An LDP entity is uniquely identified by an LDP identifier that consists of the `mplsLdpEntityLdpId` and the `mplsLdpEntityIndex` (see [Figure 1](#)).

- The `mplsLdpEntityLdpId` consists of the local LSR ID (four octets) and the label space ID (two octets). The label space ID identifies a specific label space available within the LSR.
- The `mplsLdpEntityIndex` consists of the IP address of the peer active hello adjacency, which is the 32-bit representation of the IP address assigned to the peer LSR.

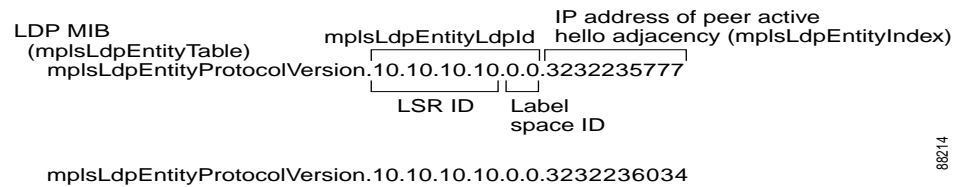
The `mplsLdpEntityProtocolVersion` is a sample object from the `mplsLdpEntityTable`.

[Figure 1](#) shows the following indexing:

- `mplsLdpEntityLdpId` = 10.10.10.10.0.0
- LSR ID = 10.10.10.10
- Label space ID = 0.0

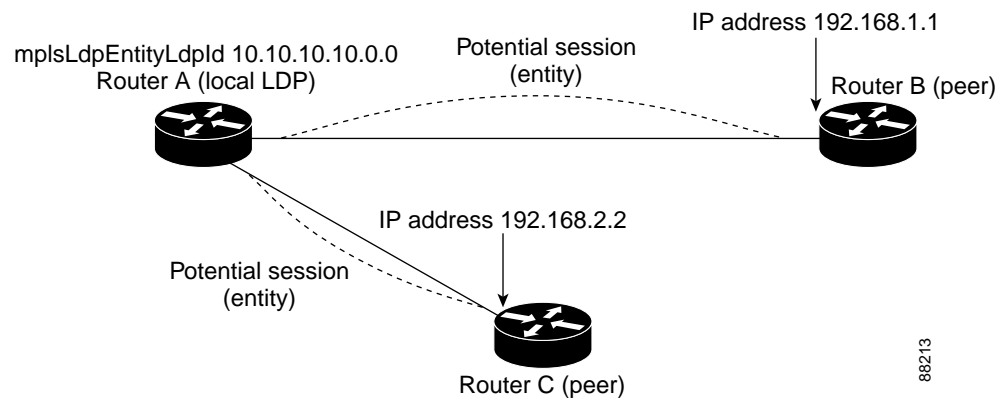
The `mplsLdpEntityLdpId` or the LDP ID consists of the LSR ID and the label space ID.

- The IP address of peer active hello adjacency or the `mplsLdpEntityIndex` = 3232235777, which is the 32-bit representation of the IP address assigned to the peer's active hello adjacency.

**Figure 1 Sample Indexing for an LDP Entity**

An LDP entity represents a label space that has the potential for a session with an LDP peer. An LDP entity is set up when a hello adjacency receives a hello message from an LDP peer.

In [Figure 2](#), Router A has potential sessions with two remote peers, Routers B and C. The mplsLdpEntityLdpId is 10.10.10.10.0.0, and the IP address of the peer active hello adjacency (mplsLdpEntityIndex) is 3232235777, which is the 32-bit representation of the IP address 192.168.1.1 for Router B.

**Figure 2 LDP Entity**

## LDP Sessions and Peers

LDP sessions exist between local entities and remote peers for the purpose of distributing label spaces. There is always a one-to-one correspondence between an LDP peer and an LDP session. A single LDP session is an LDP instance that communicates across one or more network links with a single LDP peer.

LDP supports the following types of sessions:

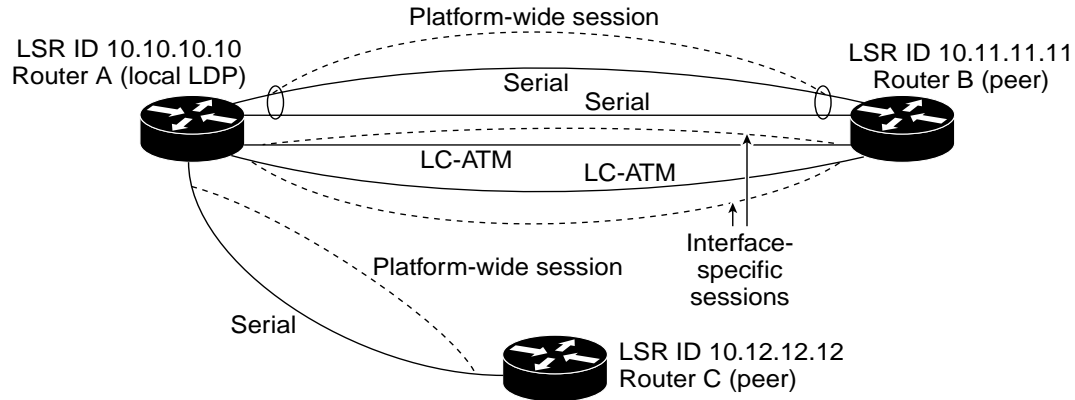
- **Interface-specific**—An interface-specific session uses interface resources for label space distributions. For example, each label-controlled ATM (LC-ATM) interface uses its own VPIs/VCIs for label space distributions. Depending on its configuration, an LDP platform can support zero, one, or more interface-specific sessions. Each LC-ATM interface has its own interface-specific label space and a nonzero label space ID.
- **Platform-wide**—An LDP platform supports a single platform-wide session for use by all interfaces that can share the same global label space. For Cisco platforms, all interface types except LC-ATM use the platform-wide session and have a label space ID of zero.

When a session is established between two peers, entries are created in the mplsLdpPeerTable and the mplsLdpSessionTable because they have the same indexing.



In Figure 3, Router A has two remote peers, Routers B and C. Router A has a single platform-wide session that consists of two serial interfaces with Router B and another platform-wide session with Router C. Router A also has two interface-specific sessions with Router B.

**Figure 3 LDP Sessions**



88215

Figure 4 shows entries that correspond to the `mplsLdpPeerTable` and the `mplsLdpSessionTable` in Figure 3.

In Figure 4, `mplsLdpSesState` is a sample object from the `mplsLdpSessionTable` on Router A. There are four `mplsLdpSesState` sample objects shown (top to bottom). The first object represents a platform-wide session associated with two serial interfaces. The next two objects represent interface-specific sessions for the LC-ATM interfaces on Routers A and B. These interface-specific sessions have nonzero peer label space IDs. The last object represents a platform-wide session for the next peer, Router C.

The indexing is based on the entries in the `mplsLdpEntityTable`. It begins with the indexes of the `mplsLdpEntityTable` and adds the following:

- Peer LDP ID = 10.11.11.11.0.0  
The peer LDP ID consists of the peer LSR ID (four octets) and the peer label space ID (two octets).
- Peer LSR ID = 10.11.11.11
- Peer label space ID = 0.0  
The peer label space ID identifies a specific peer label space available within the LSR.

**Figure 4 Sample Indexing for an LDP Session**

mplsLdpSessionTable		Peer LDP ID	
mplsLdpSesState.10.10.10.10.0.0.3232235777	Indexing of mplsLdpEntityTable	10.11.11.11.0.0	
		Peer LSR ID	Peer label space ID
		mplsLdpSesState.10.10.10.10.0.0.3232236034.10.12.12.12.0.0	
		mplsLdpSesState.10.10.10.10.0.1.3232235778.10.11.11.11.0.1	
		mplsLdpSesState.10.10.10.10.0.2.3232235779.10.11.11.11.0.2	

88216

88216

## LDP Hello Adjacencies

An LDP hello adjacency is a network link between a router and its peers. An LDP hello adjacency enables two adjacent peers to exchange label binding information.

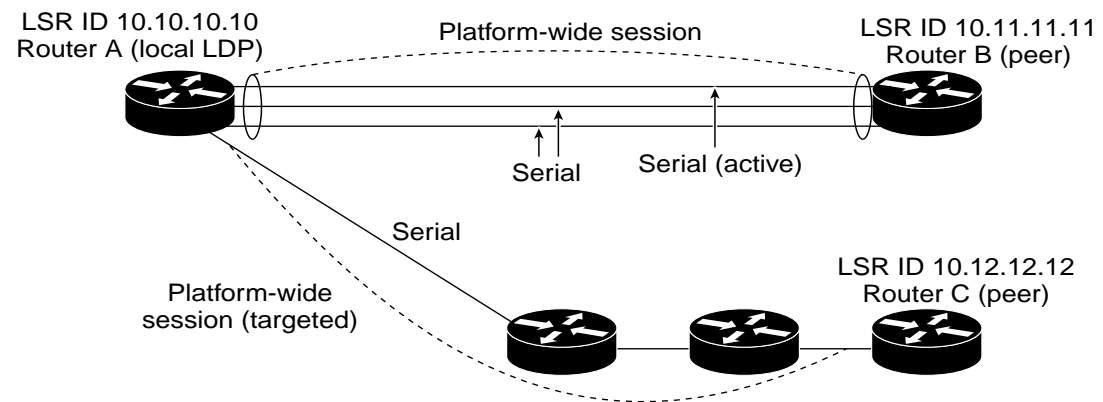
An LDP hello adjacency exists for each link on which LDP runs. Multiple LDP hello adjacencies exist whenever there is more than one link in a session between a router and its peer, such as in a platform-wide session.

A hello adjacency is considered active if it is currently engaged in a session, or nonactive if it is not currently engaged in a session.

A targeted hello adjacency is not directly connected to its peer and has an unlimited number of hops between itself and its peer. A linked hello adjacency is directly connected between two routers.

In [Figure 5](#), Router A has two remote peers, Routers B and C. Router A has a platform-wide session with Router B that consists of three serial interfaces, one of which is active and another platform-wide (targeted) session with Router C.

**Figure 5** Hello Adjacency



88217

[Figure 6](#) shows entries in the `mplsLdpHelloAdjacencyTable`. There are four `mplsLdpHelloAdjHoldTimeRem` sample objects (top to bottom). They represent the two platform-wide sessions and the four serial links shown in [Figure 5](#).

The indexing is based on the `mplsLdpSessionTable`. When the `mplsLdpHelloAdjIndex` enumerates the different links within a single session, the active link is `mplsLdpHelloAdjIndex = 1`.

**Figure 6** Sample Indexing for an LDP Hello Adjacency

```

mplsLdpHelloAdjacencyTable
  mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.1
                                     Indexing of mplsLdpSessionTable      mplsLdpHelloAdjIndex
  mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.2
  mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.3
  mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232236034.10.12.12.12.0.0.1

```

88218

## Events Generating MPLS LDP MIB Notifications in MPLS LDP MIB Version 8 Upgrade

When you enable MPLS LDP MIB notification functionality by issuing the **snmp-server enable traps mpls ldp** command, notification messages are generated and sent to a designated NMS in the network to signal the occurrence of specific events within Cisco IOS.

The MPLS LDP MIB objects involved in LDP status transitions and event notifications include the following:

- **mplsLdpSessionUp**—This message is generated when an LDP entity (a local LSR) establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).
- **mplsLdpSessionDown**—This message is generated when an LDP session between a local LSR and its adjacent LDP peer is terminated.
- **mplsLdpPathVectorLimitMismatch**—This message is generated when a local LSR establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.

The value of the path vector limit can range from 0 through 255; a value of 0 indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

We recommend that all LDP-enabled routers in the network be configured with the same path vector limit. Accordingly, the **mplsLdpPathVectorLimitMismatch** object exists in the MPLS LDP MIB to provide a warning message to the NMS when two routers engaged in LDP operations have different path vector limits.




---

**Note** This notification is generated only if the distribution method is downstream-on-demand.

---

- **mplsLdpFailedInitSessionThresholdExceeded**—This message is generated when a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented and cannot be changed.

Eight failed attempts to establish an LDP session between a local LSR and an LDP peer, due to any type of incompatibility between the devices, causes this notification message to be generated. Cisco routers support the same features across multiple platforms.

Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers try eight times to create an LDP session between themselves before the **mplsLdpFailedInitSessionThresholdExceeded** notification is generated and sent to the NMS as an informational message.

The LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight-retry threshold is exceeded.

In such cases, the LDP threshold exceeded notification alerts the network administrator about a condition in the network that might warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network.

Among such incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted above) or nonoverlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar types of LDP feature support

# MIB Tables in MPLS LDP MIB Version 8 Upgrade

Version 8 of the MPLS LDP MIB consists of the following tables:

- **mplsLdpEntityTable** ([Table 1](#))—Contains entries for every active LDP hello adjacency. Nonactive hello adjacencies appear in the **mplsLdpHelloAdjacencyTable**, rather than this table. This table is indexed by the local LDP identifier for the interface and the IP address of the peer active hello adjacency. (See [Figure 1](#).)

The advantage of showing the active hello adjacency instead of sessions in this table is that the active hello adjacency can exist even if an LDP session is not active (cannot be established). Previous implementations of the IETF MPLS-LDP MIB used sessions as the entries in this table. This approach was inadequate because as sessions went down, the entries in the entity table would disappear completely because the agent code could no longer access them. This resulted in the MIB failing to provide information about failed LDP sessions.

Directed adjacencies are also shown in this table. These entries, however, are always up administratively (**adminStatus**) and operationally (**operStatus**), because the adjacencies disappear if the directed session fails. Nondirected adjacencies might disappear from the MIB on some occasions, because adjacencies are deleted if the underlying interface becomes operationally down, for example.

- **mplsLdpEntityConfGenLRTTable** ([Table 2](#))—Contains entries for every LDP-enabled interface that is in the global label space. (For Cisco, this applies to all interfaces except LC-ATM. LC-ATM entities are shown in the **mplsLdpEntityConfAtmLRTTable** instead.) Indexing is the same as it is for the **mplsLdpEntityTable**, except two indexes have been added, **mplsLdpEntityConfGenLRMin** and **mplsLdpEntityConfGenLRMax**. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one global label range is allowed.
- **mplsLdpEntityAtmParmsTable** ([Table 3](#))—Contains entries for every LDP-enabled LC-ATM interface. This table is indexed the same as the **mplsLdpEntityTable** although only LC-ATM interfaces are shown.
- **mplsLdpEntityConfAtmLRTTable** ([Table 4](#))—Contains entries for every LDP-enabled LC-ATM interface. Indexing is the same as it is for the **mplsLdpEntityTable**, except two indexes have been added, **mplsLdpEntityConfAtmLRMinVpi** and **mplsLdpEntityConfAtmLRMinVci**. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one label range per LC-ATM interface is allowed.
- **mplsLdpEntityStatsTable** ([Table 5](#))—Augments the **mplsLdpEntityTable** and shares the exact same indexing for performing GET and GETNEXT operations. This table shows additional statistics for entities.
- **mplsLdpPeerTable** ([Table 6](#))—Contains entries for all peer sessions. This table is indexed by the local LDP identifier of the session, the IP address of the peer active hello adjacency, and the peer's LDP identifier. (See [Figure 4](#).)
- **mplsLdpHelloAdjacencyTable** ([Table 7](#))—Contains entries for all hello adjacencies. This table is indexed by the local LDP identifier of the associated session, the IP address of the peer active hello adjacency, the LDP identifier for the peer, and an arbitrary index that is set to the list position of the adjacency. (See [Figure 6](#).)
- **mplsLdpSessionTable** ([Table 8](#))—Augments the **mplsLdpPeerTable** and shares the same indexing for performing GET and GETNEXT operations. This table shows all sessions.

- `mplsLdpAtmSesTable` (Table 9)—Contains entries for LC-ATM sessions. Indexing is the same as it is for the `mplsLdpPeerTable`, except two indexes have been added, `mplsLdpSesAtmLRLowerBoundVpi` and `mplsLdpSesAtmLRLowerBoundVci`. These additional indexes allow more than one label range to be defined. However, in the current Cisco IOS implementation, only one label range per LC-ATM interface is allowed.
- `mplsLdpSesStatsTable` (Table 10)—Augments the `mplsLdpPeerTable` and shares the exact same indexing for performing GET and GETNEXT operations. This table shows additional statistics for sessions.

## mplsLdpEntityTable

Table 1 lists the `mplsLdpEntityTable` objects and their descriptions.

**Table 1** *mplsLdpEntityTable Objects and Descriptions*

Object	Description
<code>mplsLdpEntityEntry</code>	Represents an LDP entity, which is a potential session between two peers.
<code>mplsLdpEntityLdpId</code>	The LDP identifier (not accessible) consists of the local LSR ID (four octets) and the label space ID (two octets).
<code>mplsLdpEntityIndex</code>	A secondary index that identifies this row uniquely. It consists of the IP address of the peer active hello adjacency, which is the 32-bit representation of the IP address assigned to the LSR (not accessible).
<code>mplsLdpEntityProtocolVersion</code>	The version number of the LDP protocol to be used in the session initialization message.
<code>mplsLdpEntityAdminStatus</code>	The administrative status of this LDP entity is always up. If the hello adjacency fails, this entity disappears from the <code>mplsLdpEntityTable</code> .
<code>mplsLdpEntityOperStatus</code>	The operational status of this LDP entity. Values are unknown(0), enabled(1), and disabled(2).
<code>mplsLdpEntityTcpDscPort</code>	The TCP discovery port for LDP or TDP. The default value is 646 (LDP).
<code>mplsLdpEntityUdpDscPort</code>	The UDP discovery port for LDP or TDP. The default value is 646 (LDP).
<code>mplsLdpEntityMaxPduLength</code>	The maximum PDU length that is sent in the common session parameters of an initialization message.
<code>mplsLdpEntityKeepAliveHoldTimer</code>	The two-octet value that is the proposed keepalive hold time for this LDP entity.
<code>mplsLdpEntityHelloHoldTimer</code>	The two-octet value that is the proposed hello hold time for this LDP entity.
<code>mplsLdpEntityInitSesThreshold</code>	The threshold for notification when this entity and its peer are engaged in an endless sequence of initialization messages. The default value is 8 and cannot be changed by SNMP or CLI.

**Table 1** *mplsLdpEntityTable Objects and Descriptions (continued)*

Object	Description
mplsLdpEntityLabelDistMethod	The specified method of label distribution for any given LDP session. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).
mplsLdpEntityLabelRetentionMode	Can be configured to use either conservative(1) for LC-ATM or liberal(2) for all other interfaces.
mplsLdpEntityPVLMisTrapEnable	<p>Indicates whether the mplsLdpPVLMismatch trap should be generated.</p> <p>If the value is enabled(1), the trap is generated. If the value is disabled(2), the trap is not generated. The default is disabled(2).</p> <p><b>Note</b> The mplsLdpPVLMismatch trap is generated only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>
mplsLdpEntityPVL	<p>If the value of this object is 0, loop detection for path vectors is disabled. Otherwise, if this object has a value greater than zero, loop detection for path vectors is enabled, and the path vector limit is this value.</p> <p><b>Note</b> The mplsLdpEntityPVL object is non-zero only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>
mplsLdpEntityHopCountLimit	<p>If the value of this object is 0, loop detection using hop counters is disabled.</p> <p>If the value of this object is greater than 0, loop detection using hop counters is enabled, and this object specifies this entity's maximum allowable value for the hop count.</p> <p><b>Note</b> The mplsLdpEntityHopCountLimit object is non-zero only if mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>
mplsLdpEntityTargPeer	If this LDP entity uses a targeted adjacency, this object is set to true(1). The default value is false(2).
mplsLdpEntityTargPeerAddrType	The type of the internetwork layer address used for the extended discovery. This object indicates how the value of mplsLdpEntityTargPeerAddr is to be interpreted.
mplsLdpEntityTargPeerAddr	The value of the internetwork layer address used for the targeted adjacency.
mplsLdpEntityOptionalParameters	<p>Specifies the optional parameters for the LDP initialization message. If the value is generic(1), no optional parameters are sent in the LDP initialization message associated with this entity.</p> <p>LC-ATM uses atmParameters(2) to specify that a row in the mplsLdpEntityAtmParmsTable corresponds to this entry.</p> <p><b>Note</b> Frame Relay parameters are not supported.</p>

**Table 1** *mplsLdpEntityTable Objects and Descriptions (continued)*

Object	Description
mplsLdpEntityDiscontinuityTime	The value of sysUpTime on the most recent occasion when one or more of this entity's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpEntityStatsTable that are associated with this entity. If no such discontinuities have occurred since the last reinitialization of the local management subsystem, this object contains a 0 value.
mplsLdpEntityStorType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityRowStatus	This object is a read-only implementation that is always active.

## mplsLdpEntityConfGenLRTable

Table 2 lists the mplsLdpEntityConfGenLRTable objects and their descriptions.

**Table 2** *mplsLdpEntityConfGenLRTable Objects and Descriptions*

Object	Description
mplsLdpEntityConfGenLREntry	A row in the LDP Entity Configurable Generic Label Range table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary (VPI/VCI pair) and a lower boundary (VPI/VCI pair).  The current implementation supports one label range per entity.
mplsLdpEntityConfGenLRMin	The minimum label configured for this range (not accessible).
mplsLdpEntityConfGenLRMax	The maximum label configured for this range (not accessible).
mplsLdpEntityConfGenIfIndxOrZero	This value represents the SNMP IF-MIB index for the platform-wide entity. If the active hello adjacency is targeted, the value is 0.
mplsLdpEntityConfGenLRStorType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityConfGenLRRowStatus	This object is a read-only implementation that is always active.

## mplsLdpEntityAtmParmsTable

Table 3 lists the mplsLdpEntityAtmParmsTable objects and their descriptions.

**Table 3** *mplsLdpEntityAtmParmsTable Objects and Descriptions*

Object	Description
mplsLdpEntityAtmParmsEntry	Represents the ATM parameters and ATM information for this LDP entity.
mplsLdpEntityAtmIfIndxOrZero	This value represents the SNMP IF-MIB index for the interface-specific LC-ATM entity.
mplsLdpEntityAtmMergeCap	Denotes the merge capability of this entity.
mplsLdpEntityAtmLRComponents	Number of label range components in the initialization message. This also represents the number of entries in the mplsLdpEntityConfAtmLRTable that correspond to this entry.
mplsLdpEntityAtmVcDirectionality	<p>If the value of this object is <code>bidirectional(0)</code>, a given VCI within a given VPI is used as a label for both directions independently of one another.</p> <p>If the value of this object is <code>unidirectional(1)</code>, a given VCI within a VPI designates one direction.</p>
mplsLdpEntityAtmLsrConnectivity	<p>The peer LSR can be connected indirectly by means of an ATM VP, so that the VPI values can be different on the endpoints. For that reason, the label must be encoded entirely within the VCI field.</p> <p>Values are <code>direct(1)</code>, the default, and <code>indirect(2)</code>.</p>
mplsLdpEntityDefaultControlVpi	The default VPI value for the non-MPLS connection.
mplsLdpEntityDefaultControlVci	The default VCI value for the non-MPLS connection.
mplsLdpEntityUnlabTrafVpi	VPI value of the VCC supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.
mplsLdpEntityUnlabTrafVci	VCI value of the VCC supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.
mplsLdpEntityAtmStorType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityAtmRowStatus	This object is a read-only implementation that is always active.

## mplsLdpEntityConfAtmLRTable

Table 4 lists the mplsLdpEntityConfAtmLRTable objects and their descriptions.



**Table 4** *mplsLdpEntityConfAtmLRTable Objects and Descriptions*

Object	Description
mplsLdpEntityConfAtmLREntry	A row in the LDP Entity Configurable ATM Label Range Table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary (VPI/VCI pair) and a lower boundary (VPI/VCI pair). This is the same data used in the initialization message. This label range should overlap the label range of the peer.
mplsLdpEntityConfAtmLRMinVpi	The minimum VPI number configured for this range (not accessible).
mplsLdpEntityConfAtmLRMinVci	The minimum VCI number configured for this range (not accessible).
mplsLdpEntityConfAtmLRMaxVpi	The maximum VPI number configured for this range (not accessible).
mplsLdpEntityConfAtmLRMaxVci	The maximum VCI number configured for this range (not accessible).
mplsLdpEntityConfAtmLRStorType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityConfAtmLRRowStatus	This object is a read-only implementation that is always active.

## mplsLdpEntityStatsTable

Table 5 lists the mplsLdpEntityStatsTable objects and their descriptions.

**Table 5** *mplsLdpEntityStatsTable Objects and Descriptions*

Object	Description
mplsLdpEntityStatsEntry	These entries augment the mplsLdpEntityTable by providing additional information for each entry.
mplsLdpAttemptedSessions	Not supported in this feature.
mplsLdpSesRejectedNoHelloErrors	A count of the session rejected/no hello error notification messages sent or received by this LDP entity.
mplsLdpSesRejectedAdErrors	A count of the session rejected/parameters advertisement mode error notification messages sent or received by this LDP entity.
mplsLdpSesRejectedMaxPduErrors	A count of the session rejected/parameters max PDU length error notification messages sent or received by this LDP entity.
mplsLdpSesRejectedLRErrors	A count of the session rejected/parameters label range notification messages sent or received by this LDP entity.
mplsLdpBadLdpIdentifierErrors	A count of the number of bad LDP identifier fatal errors detected by the session associated with this LDP entity.

**Table 5** *mplsLdpEntityStatsTable Objects and Descriptions (continued)*

Object	Description
mplsLdpBadPduLengthErrors	A count of the number of bad PDU length fatal errors detected by the session associated with this LDP entity.
mplsLdpBadMessageLengthErrors	A count of the number of bad message length fatal errors detected by the session associated with this LDP entity.
mplsLdpBadTlvLengthErrors	A count of the number of bad Type-Length-Value (TLV) length fatal errors detected by the session associated with this LDP entity.
mplsLdpMalformedTlvValueErrors	A count of the number of malformed TLV value fatal errors detected by the session associated with this LDP entity.
mplsLdpKeepAliveTimerExpErrors	A count of the number of session keepalive timer expired errors detected by the session associated with this LDP entity.
mplsLdpShutdownNotifReceived	A count of the number of shutdown notifications received related to the session associated with this LDP entity.
mplsLdpShutdownNotifSent	A count of the number of shutdown notifications sent related to the session associated with this LDP entity.

## mplsLdpPeerTable

Table 6 lists the mplsLdpPeerTable objects and their descriptions.

**Table 6** *mplsLdpPeerTable Objects and Descriptions*

Object	Description
mplsLdpPeerEntry	Information about a single peer that is related to a session (not accessible). <b>Note</b> This table is augmented by the mplsLdpSessionTable.
mplsLdpPeerLdpId	The LDP identifier of this LDP peer (not accessible) consists of the peer LSR ID (four octets) and the peer label space ID (two octets).
mplsLdpPeerLabelDistMethod	For any given LDP session, the method of label distribution. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).

**Table 6** *mplsLdpPeerTable Objects and Descriptions (continued)*

Object	Description
mplsLdpPeerLoopDetectionForPV	<p>An indication of whether loop detection based on path vectors is disabled or enabled for this peer.</p> <p>For downstream unsolicited distribution (mplsLdpPeerLabelDistMethod is downstreamUnsolicited(2)), this object always has a value of disabled(0) and loop detection is disabled.</p> <p>For downstream-on-demand distribution (mplsLdpPeerLabelDistMethod is downstreamOnDemand(1)), this object has a value of enabled(1), provided that loop detection based on path vectors is enabled.</p>
mplsLdpPeerPVL	<p>If the value of mplsLdpPeerLoopDetectionForPV for this entry is enabled(1), this object represents that path vector limit for this peer.</p> <p>If the value of mplsLdpPeerLoopDetectionForPV for this entry is disabled(0), this value should be 0.</p>

## mplsLdpHelloAdjacencyTable

Table 7 lists the mplsLdpHelloAdjacencyTable objects and their descriptions.

**Table 7** *mplsLdpHelloAdjacencyTable Objects and Descriptions*

Object	Description
mplsLdpHelloAdjacencyEntry	Each row represents a single LDP hello adjacency. An LDP session can have one or more hello adjacencies (not accessible).
mplsLdpHelloAdjIndex	An identifier for this specific adjacency (not accessible). The active hello adjacency has mplsLdpHelloAdjIndex equal to 1.
mplsLdpHelloAdjHoldTimeRem	The time remaining for this hello adjacency. This interval changes when the next hello message, which corresponds to this hello adjacency, is received.
mplsLdpHelloAdjType	This adjacency is the result of a link hello if the value of this object is link(1). Otherwise, this adjacency is a result of a targeted hello and its value is targeted(2).

## mplsLdpSessionTable

Table 8 lists the mplsLdpSessionTable objects and their descriptions.

**Table 8** *mplsLdpSessionTable Objects and Descriptions*

Object	Description
mplsLdpSessionEntry	An entry in this table represents information on a single session between an LDP entity and an LDP peer. The information contained in a row is read-only. This table augments the mplsLdpPeerTable.
mplsLdpSesState	<p>The current state of the session. All of the states are based on the LDP or TDP state machine for session negotiation behavior.</p> <p>The states are as follows:</p> <ul style="list-style-type: none"> <li>• nonexistent(1)</li> <li>• initialized(2)</li> <li>• openrec(3)</li> <li>• opensent(4)</li> <li>• operational(5)</li> </ul>
mplsLdpSesProtocolVersion	The version of the LDP protocol which this session is using. This is the version of the LDP protocol that has been negotiated during session initialization.
mplsLdpSesKeepAliveHoldTimeRem	The keepalive hold time remaining for this session.
mplsLdpSesMaxPduLen	The value of maximum allowable length for LDP PDUs for this session. This value could have been negotiated during the session initialization.
mplsLdpSesDiscontinuityTime	<p>The value of sysUpTime on the most recent occasion when one or more of this session's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpSesStatsTable associated with this session.</p> <p>The initial value of this object is the value of sysUpTime when the entry was created in this table.</p>

## mplsLdpAtmSesTable

Table 9 lists the mplsLdpAtmSesTable objects and their descriptions.

**Table 9** *mplsLdpAtmSesTable Objects and Descriptions*

Objects	Description
mplsLdpAtmSesEntry	An entry in this table represents information on a single label range intersection between an LDP entity and an LDP peer (not accessible).
mplsLdpAtmSesLRLowerBoundVpi	The minimum VPI number for this range (not accessible).
mplsLdpAtmSesLRLowerBoundVci	The minimum VCI number for this range (not accessible).

**Table 9** *mplsLdpAtmSesTable Objects and Descriptions (continued)*

Objects	Description
mplsLdpAtmSesLRUpperBoundVpi	The maximum VPI number for this range (read-only).
mplsLdpAtmSesLRUpperBoundVci	The maximum VCI number for this range (read-only).

## mplsLdpSesStatsTable

[Table 10](#) lists the mplsLdpSesStatsTable objects and their descriptions.

**Table 10** *mplsLdpSesStatsTable Objects and Descriptions*

Object	Description
mplsLdpSesStatsEntry	An entry in this table represents statistical information on a single session between an LDP entity and an LDP peer. This table augments the mplsLdpPeerTable.
mplsLdpSesStatsUnkMesTypeErrors	This object is the count of the number of unknown message type errors detected during this session.
mplsLdpSesStatsUnkTlvErrors	This object is the count of the number of unknown TLV errors detected during this session.

## VPN Contexts in MPLS LDP MIB Version 8 Upgrade

Within an MPLS Border Gateway Protocol (BGP) 4 Virtual Private Network (VPN) environment, separate LDP processes can be created for each VPN. These processes and their associated data are called LDP contexts. Each context is independent from all others and contains data specific only to that context.

Cisco IOS Release 12.0(11)ST and later releases include the VPN Aware LDP MIB feature that allows the LDP MIB to get VPN context information. The feature adds support for different contexts for different MPLS VPNs. Users of the MIB can view MPLS LDP processes for a given MPLS VPN. The VPN Aware LDP MIB feature does not change the syntax of the IETF MPLS-LDP MIB. It changes the number and types of entries within the tables.

The IETF MPLS-LDP MIB can show information about only one context at a time. You can specify a context, either a global context or an MPLS VPN context, using an SNMP security name.

The following sections describe topics related to the VPN Aware LDP MIB feature:

- [SNMP Contexts, page 21](#)
- [VPN Aware LDP MIB Sessions, page 21](#)
- [VPN Aware LDP MIB Notifications, page 23](#)

## SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

VPN-aware SNMP requires that SNMP manager and agent entities operating in a VPN environment agree on mapping between the SNMP security name and the VPN name. This mapping is created by using different contexts for the SNMP data of different VPNs, which is accomplished through the configuration of the SNMP View-based Access Control Model MIB (SNMP-VACM-MIB). The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space within the context of only that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values within a VPN context:

- The first security phase is authentication of the username. During this phase, the user is authorized for SNMP access.
- The second phase is access control. During this phase, the user is authorized for SNMP access to the group objects in the requested SNMP context.
- In the third phase, the user can access a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

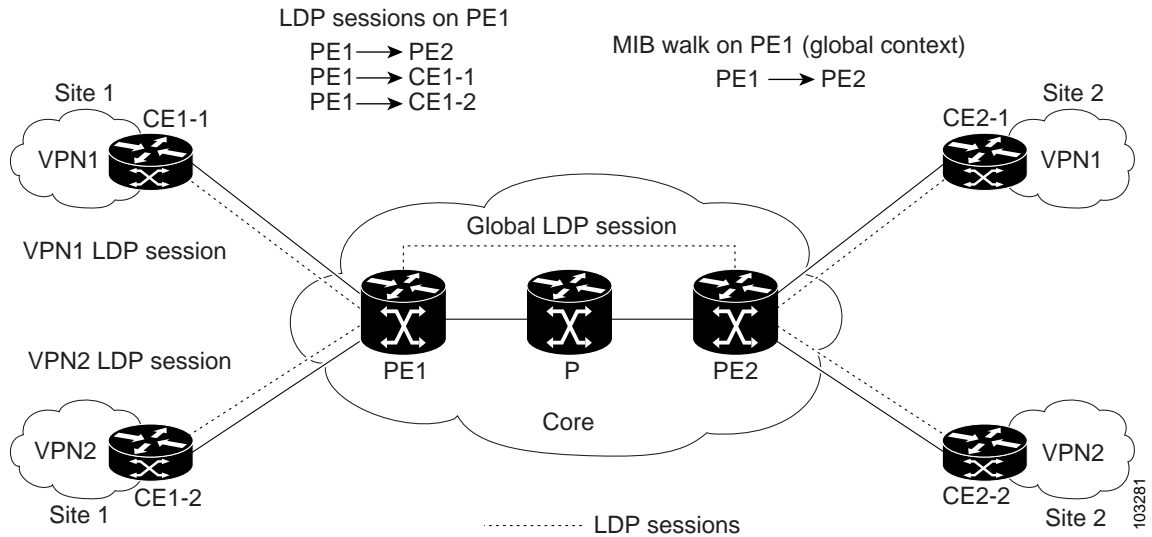
IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VRF instances and SNMP community strings. When a VRF instance is associated with an SNMP community string, SNMP processes requests coming in for a particular community string only if they are received from the configured VRF. If the community string contained in the incoming packet does not have a VRF associated with it, it is processed only if it came in through a non-VRF interface.

You can also enable or disable authentication traps for SNMP packets dropped due to VRF mismatches. By default, if SNMP authentication traps are enabled, VRF authentication traps are also enabled.

## VPN Aware LDP MIB Sessions

Prior to Cisco IOS Release 12.0(11)ST, an SNMP query to the MPLS LDP MIB returned information about global sessions only. A query did not return information about LDP sessions in a VPN context. The IETF MPLS LDP MIB retrieved information from global routing tables, but did not retrieve information from VPN routing and forwarding instances (VRFs) that store per-VPN routing data. The MPLS LDP MIB looked only at LDP processes in the global context and ignored all other sessions. A query on a VRF returned no information. You can view LDP processes in a VPN context.

[Figure 7](#) shows a sample MPLS VPN network with the MPLS LDP sessions prior to the implementation of the VPN Aware LDP MIB feature.

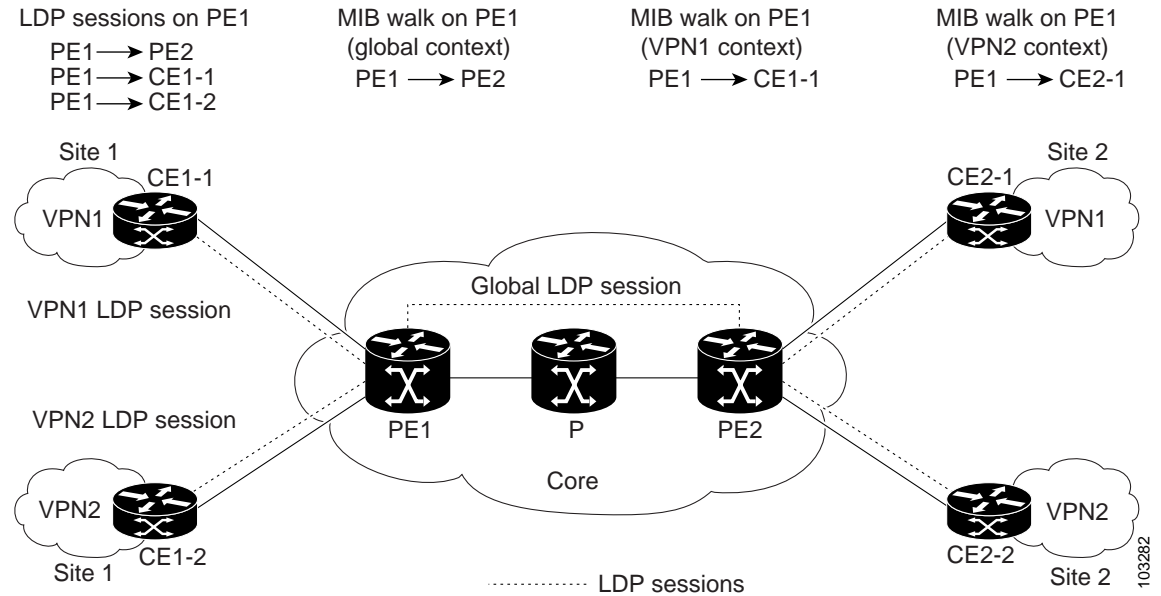
**Figure 7** *MPLS LDP Sessions Setup Before VPN Aware LDP MIB Feature*

A MIB walk prior to this Cisco IOS release displayed only global session information.

With the VPN Aware LDP MIB enhancement in this Cisco IOS release, an SNMP query to the IETF MPLS-LDP-MIB supports both global and VPN contexts. This feature allows you to enter LDP queries on any VRF and on the core (global context). A query can differentiate between LDP sessions from different VPNs. LDP session information for a VPN stays in the context of that VPN. Therefore, the information from one VPN is not available to a user of a different VPN. The VPN Aware update to the LDP MIB also allows you to view LDP processes operating in a Carrier Supporting Carrier (CSC) network.

In an MPLS VPN, a service provider edge router (PE) might contain VRFs for several VPNs as well as a global routing table. To set up separate LDP processes for different VPNs on the same device, you need to configure each VPN with a unique securityName, contextName, and View-based Access Control Model (VACM) view. The VPN securityName must be configured for the IETF MPLS LDP MIB.

Figure 8 shows LDP sessions for a sample MPLS VPN network with the VPN Aware LDP MIB feature.

**Figure 8 MPLS LDP Sessions with the VPN Aware LDP MIB Feature**

With the VPN Aware LDP MIB feature, you can do MIB queries or MIB walks for an MPLS VPN LDP session or a global LDP session.

**Note**

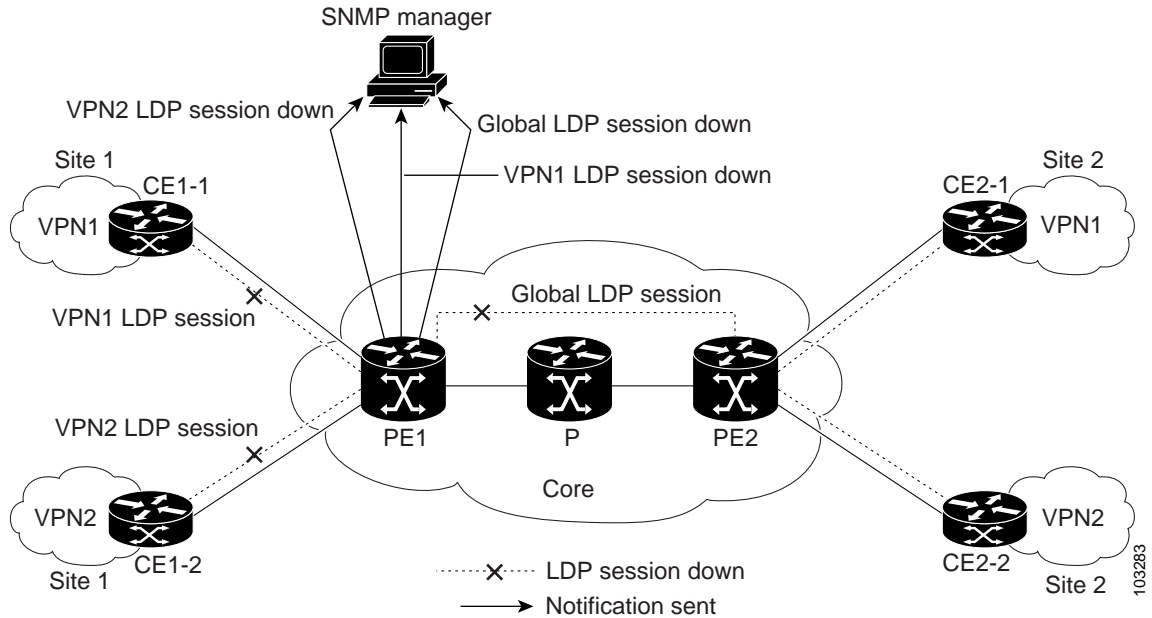
To verify LDP session information for a specific VPN, use the **show mpls ldp neighbor vrf vpn-name detail** command.

## VPN Aware LDP MIB Notifications

Prior to Cisco IOS Release 12.0(11)ST, all notification messages for MPLS LDP sessions were sent to the same designated network management station (NMS) in the network. The notifications were enabled with the **snmp-server enable traps mpls ldp** command.

Figure 9 shows LDP notifications that were sent before the implementation of the VPN Aware LDP MIB feature.



**Figure 9** *LDP Notifications Sent Before the VPN Aware LDP MIB Feature*

The VPN Aware LDP MIB feature supports LDP notifications for multiple LDP contexts for VPNs. LDP notifications can be generated for the core (global context) and for different VPNs. You can cause notifications be sent to different NMS hosts for different LDP contexts. LDP notifications associated with a specific VRF are sent to the NMS designated for that VRF. LDP global notifications are sent to the NMS configured to receive global traps.

To enable LDP context notifications for the VPN Aware LDP MIB feature, use either the SNMP object `mplsLdpSessionsUpDownEnable` (in the global LDP context only) or the following extended global configuration commands.

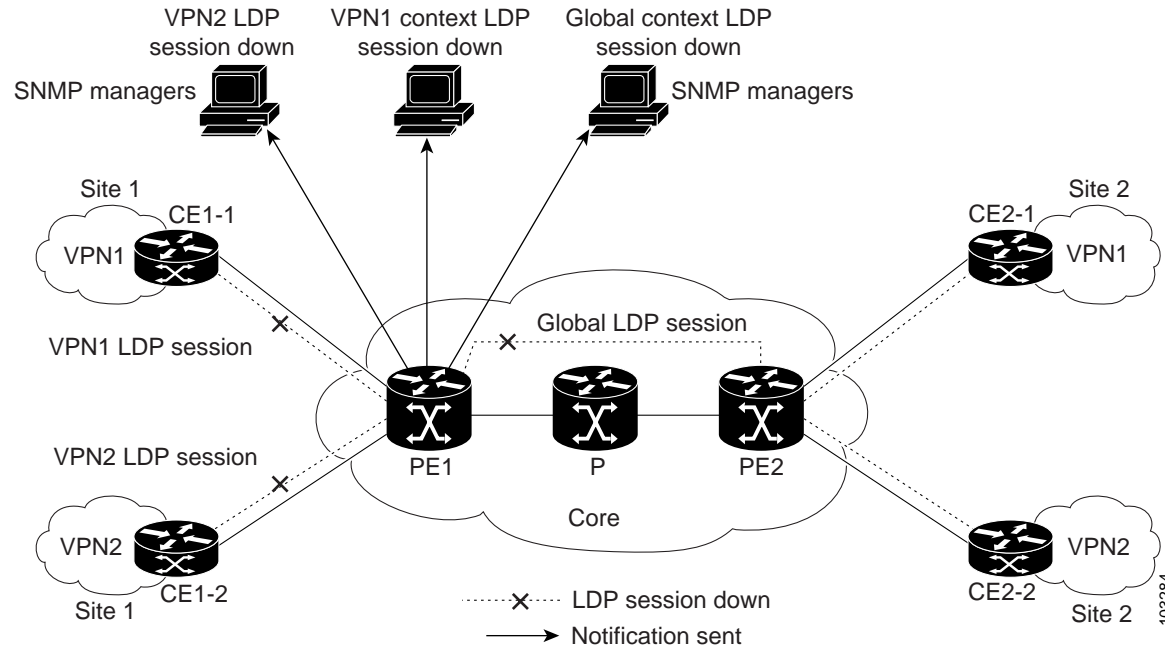
To enable LDP notifications for the global context, use the following commands:

```
PE-Router(config)# snmp-server host host-address traps community mpls-ldp
PE-Router(config)# snmp-server enable traps mpls ldp
```

To enable LDP notifications for a VPN context, use the following commands:

```
PE-Router(config)# snmp-server host host-address vrf vrf-name version {v1|v2c|v3}
community community-string udp-port upd-port mpls-ldp
PE-Router(config)# snmp-server enable traps mpls ldp
```

Figure 10 shows LDP notifications with the VPN Aware LDP MIB feature.

**Figure 10** *LDP Notifications With the VPN Aware LDP MIB Feature*

## How to Configure MPLS LDP MIB Version 8 Upgrade

This section contains the following procedures:

- [Enabling the SNMP Agent, page 25](#) (required)
- [Enabling Cisco Express Forwarding, page 26](#) (required)
- [Enabling MPLS Globally, page 27](#) (required)
- [Enabling LDP Globally, page 28](#) (required)
- [Enabling MPLS on an Interface, page 29](#) (required)
- [Enabling LDP on an Interface, page 30](#) (required)
- [Configuring a VPN Aware LDP MIB, page 31](#) (required)
- [Verifying MPLS LDP MIB Version 8 Upgrade, page 37](#) (optional)

### Enabling the SNMP Agent

Perform this task to enable the SNMP agent.

#### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community *string* [view *view-name*] [ro] [number]**

5. **end**
6. **write memory**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.  If no SNMP information is displayed, continue with the next step.  If any SNMP information is displayed, you can modify the information or change it as desired.
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>snmp-server community string [view view-name] [ro] [number]</b>  <b>Example:</b> Router(config)# snmp-server community public ro	Configures read-only (ro) community strings for the MPLS LDP MIB. <ul style="list-style-type: none"> <li>The <i>string</i> argument functions like a password, permitting access to SNMP functionality on label switch routers (LSRs) in an MPLS network.</li> <li>The optional <b>ro</b> keyword configures read-only (ro) access to the objects in the MPLS LDP MIB.</li> </ul>
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.
Step 6	<b>write memory</b>  <b>Example:</b> Router# write memory	Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.

## Enabling Cisco Express Forwarding

Perform this task to enable Cisco Express Forwarding or distributed Cisco Express Forwarding.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **ip cef distributed**
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef distributed</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables distributed Cisco Express Forwarding.
Step 4	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

## Enabling MPLS Globally

Perform this task to enable MPLS globally.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls ip**
4. **end**

**DETAILED STEPS**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>mpls ip</b>  <b>Example:</b> Router(config)# mpls ip	Enables MPLS forwarding of IPv4 packets along normally routed paths for the platform.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

**Enabling LDP Globally**

Perform this task to enable LDP globally.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **mpls label protocol {ldp | tdp}**
4. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode.
	<b>Example:</b> <code>Router&gt; enable</code>	<ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	<b>Example:</b> <code>Router# configure terminal</code>	
Step 3	<code>mpls label protocol {ldp   tdp}</code>	Specifies the platform default label distribution protocol.
	<b>Example:</b> <code>Router(config)# mpls label protocol ldp</code>	
Step 4	<code>end</code>	Exits to privileged EXEC mode.
	<b>Example:</b> <code>Router(config)# end</code>	

## Enabling MPLS on an Interface

Perform this task to enable MPLS on an interface.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface [type number]`
4. `mpls ip`
5. `end`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> [ <i>type number</i> ]  <b>Example:</b> Router(config)# interface Ethernet 1	Enters interface configuration mode. <ul style="list-style-type: none"> <li>The <i>type number</i> argument identifies the interface to be configured.</li> </ul>
Step 4	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Enables MPLS forwarding of IPv4 packets along normally routed paths for a particular interface.
Step 5	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits to privileged EXEC mode.

## Enabling LDP on an Interface

Perform this task to enable LDP on an interface.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** [*type number*]
4. **mpls label protocol** {ldp | tdp | both}
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> [type number]  <b>Example:</b> Router(config)# interface Ethernet 1	Enters interface configuration mode. <ul style="list-style-type: none"><li>The <i>type number</i> argument identifies the interface to be configured.</li></ul>
Step 4	<b>mpls label protocol</b> {ldp   tdp   both}  <b>Example:</b> Router(config-if)# mpls label protocol ldp	Specifies the label distribution protocol to be used on a given interface.
Step 5	<b>end</b>  <b>Example:</b> Router(config-if)# end	Exits to privileged EXEC mode.

## Configuring a VPN Aware LDP MIB

To configure a VPN Aware LDP MIB, perform the following tasks:

- [Configuring SNMP Support for a VPN, page 31](#)
- [Configuring an SNMP Context for a VPN, page 32](#)
- [Associating an SNMP VPN Context with SNMPv1 or SNMPv2, page 34](#)

## Configuring SNMP Support for a VPN

Perform this task to configure SNMP support for a Virtual Private Network (VPN) or a remote VPN.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-address* [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]]  
*community-string* [udp-port *port*] [notification-type] [vrf *vrf-name*]
4. **snmp-server engineID remote** *ip-address* [udp-port *udp-port-number*] [vrf *vrf-name*]  
*engineid-string*
5. **end**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server host</b> <i>host-address</i> [ <b>traps</b>   <b>informs</b> ] [ <b>version</b> {1   2c   3 [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}] <i>community-string</i> [ <b>udp-port</b> <i>port</i> ] [ <i>notification-type</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config)# snmp-server host example.com vrf trap-vrf	Specifies the recipient of an SNMP notification operation and specifies the Virtual Private Network (VPN) routing and forwarding (VRF) instance table to be used for the sending of SNMP notifications.
Step 4	<b>snmp-server engineID remote</b> <i>ip-address</i> [ <b>udp-port</b> <i>udp-port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ] <i>engineid-string</i>  <b>Example:</b> Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf 80000009030000B064EFE100	Configures a name for the remote SNMP engine on a router.
Step 5	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

## What to Do Next

Proceed to the [“Configuring an SNMP Context for a VPN”](#) section on page 32.

## Configuring an SNMP Context for a VPN

Perform this task to configure an SNMP context for a VPN. This sets up a unique SNMP context for a VPN, which allows you to access the VPN’s LDP session information.

## SNMP Context

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN’s specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

## VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables for a VPN. Cisco IOS adds the RD to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

Either the RD is an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter an RD in either of these formats:

- 16-bit ASN: your 32-bit number, for example, 101:3.
- 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server context** *context-name*
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **context** *context-name*
7. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server context context-name</b>  <b>Example:</b> Router(config)# snmp-server context context1	Creates and names an SNMP context.
Step 4	<b>ip vrf vrf-name</b>  <b>Example:</b> Router(config)# ip vrf vrf1	Configures a Virtual Private Network (VPN) routing and forwarding instance (VRF) table and enters VRF configuration mode.
Step 5	<b>rd route-distinguisher</b>  <b>Example:</b> Router(config-vrf)# rd 100:120	Creates a VPN route distinguisher.
Step 6	<b>context context-name</b>  <b>Example:</b> Router(config-vrf)# context context1	Associates an SNMP context with a particular VRF.
Step 7	<b>route-target {import   export   both}</b> <b>route-target-ext-community</b>  <b>Example:</b> Router(config-vrf)# route-target export 100:1000	(Optional) Creates a route-target extended community for a VRF.
Step 8	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

## What to Do Next

Proceed to the [“Associating an SNMP VPN Context with SNMPv1 or SNMPv2”](#) section on page 34.

## Associating an SNMP VPN Context with SNMPv1 or SNMPv2

Perform this task to associate an SNMP VPN context with SNMPv1 or SNMPv2. This allows you to access LDP session information for a VPN using SNMPv1 or SNMPv2.

## SNMPv1 or SNMPv2 Security

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP Versions 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP Version 3 performs.

To configure the VPN Aware LDP MIB feature when using SNMP Version 1 or SNMP Version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if they come in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, the packet is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from using a clear text community string to query the VPN data. However, this is not as secure as using SNMPv3.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote host** [**udp-port port**]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access access-list**]
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context context-name**] [**read readview**] [**write writeview**] [**notify notifyview**] [**access access-list**]
5. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
6. **snmp-server enable traps** [*notification-type*]
7. **snmp-server host** *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] [*community-string*] [**udp-port port**] [**notification-type**] [**vrf vrf-name**]
8. **snmp mib community-map** *community-name* [**context context-name**] [**engineid engine-id**] [**security-name security-name**] **target-list** *vpn-list-name*
9. **snmp mib target list** *vpn-list-name* {**vrf vrf-name** | **host ip-address**}
10. **no snmp-server trap authentication vrf**
11. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server user username group-name [remote host [udp-port port]] {v1   v2c   v3 [encrypted] [auth {md5   sha} auth-password]} [access access-list]</b>  <b>Example:</b> Router(config)# snmp-server user customer1 group1 v1	Configures a new user to an SNMP group.
Step 4	<b>snmp-server group group-name {v1   v2c   v3 {auth   noauth   priv}} [context context-name] [read readview] [write writeview] [notify notifyview] [access access-list]</b>  <b>Example:</b> Router(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1	Configures a new SNMP group or a table that maps SNMP users to SNMP views. <ul style="list-style-type: none"> <li>Use the <b>context context-name</b> keyword and argument to associate the specified SNMP group with a configured SNMP context.</li> </ul>
Step 5	<b>snmp-server view view-name oid-tree {included   excluded}</b>  <b>Example:</b> Router(config)# snmp-server view view1 ipForward included	Creates or updates a view entry.
Step 6	<b>snmp-server enable traps [notification-type]</b>  <b>Example:</b> Router(config)# snmp-server enable traps	Enables all SNMP notifications (traps or informs) available on your system.
Step 7	<b>snmp-server host host-address [traps   informs] [version {1   2c   3 [auth   noauth   priv]] [community-string [udp-port port] [notification-type] [vrf vrf-name]</b>  <b>Example:</b> Router(config)# snmp-server host 10.0.0.1 vrf customer1 public udp-port 7002	Specifies the recipient of an SNMP notification operation.

	Command or Action	Purpose
Step 8	<pre>snmp mib community-map community-name [context context-name] [engineid engine-id] [security-name security-name] target-list vpn-list-name</pre> <p><b>Example:</b> Router(config)# snmp mib community-maps community1 context context1 target-list commAVpn</p>	Associates an SNMP community with an SNMP context, Engine ID, or security name.
Step 9	<pre>snmp mib target list vpn-list-name {vrf vrf-name   host ip-address}</pre> <p><b>Example:</b> Router(config)# snmp mib target list commAVpn vrf vrfl</p>	Creates a list of target VRFs and hosts to associate with an SNMP community.
Step 10	<pre>no snmp-server trap authentication vrf</pre> <p><b>Example:</b> Router(config)# no snmp-server trap authentication vrf</p>	<p>(Optional) Disables all SNMP authentication notifications (traps and informs) generated for packets received on VRF interfaces.</p> <ul style="list-style-type: none"> <li>Use this command to disable authentication traps only for those packets on VRF interfaces with incorrect community associations.</li> </ul>
Step 11	<pre>exit</pre> <p><b>Example:</b> Router(config) exit</p>	Exits to privileged EXEC mode.

## Verifying MPLS LDP MIB Version 8 Upgrade

Perform a MIB walk using your SNMP management tool to verify that the MPLS LDP MIB Version 8 Upgrade feature is functioning.

## Configuration Examples for MPLS LDP MIB Version 8 Upgrade

This section provides the following configuration examples:

- [MPLS LDP MIB Version 8 Upgrade Examples, page 37](#)
- [Configuring a VPN Aware SNMP Context for SNMPv1 or SNMPv2: Example, page 38](#)

## MPLS LDP MIB Version 8 Upgrade Examples

The following example shows how to enable an SNMP agent on the host NMS:

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# snmp-server community
```

The following example shows how to enable SNMPv1 and SNMPv2C on the host NMS. The configuration permits any SNMP agent to access all MPLS LDP MIB objects that have read-only permission using the community string public.

```
Router(config)# snmp-server community public
```

The following example shows how to allow read-only access to all MPLS LDP MIB objects relating to members of access list 4 that specify the comaccess community string. No other SNMP agents will have access to any of the MPLS LDP MIB objects.

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to enable LDP globally and then on an interface:

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# mpls label protocol ldp
```

```
Router(config)# interface Ethernet1
```

```
Router(config-if)# mpls label protocol ldp
```

```
Router(config-if)# end
```

## Configuring a VPN Aware SNMP Context for SNMPv1 or SNMPv2: Example

The following configuration example shows how to configure a VPN Aware SNMP context for the MPLS LDP MIB Version 8 with SNMPv1 or SNMPv2:

```
snmp-server context A
snmp-server context B

ip vrf CustomerA
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!

ip vrf CustomerB
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!

interface Ethernet3/1
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 10.0.0.0 255.255.0.0

interface Ethernet3/2
 description Belongs to VPN B
 ip vrf forwarding CustomerB
 ip address 10.0.0.1 255.255.0.0
```

```
snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c

snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB

snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included

snmp-server enable traps
snmp-server host 10.0.0.3 vrf CustomerA commA udp-port 7002
snmp-server host 10.0.0.4 vrf CustomerB commB udp-port 7002

snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid
```

## Additional References

The following sections provide references related to the MPLS LDP MIB Version 8 Upgrade feature.



## Related Documents

Related Topic	Document Title
MPLS LDP configuration tasks	<a href="#">MPLS Label Distribution Protocol (LDP)</a>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB (draft-ietf-mpls-ldp-mib-08.txt)</li> <li>SNMP-VACM-MIB The View-based Access Control Model (ACM) MIB for SNMP</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFCs	Title
<p>RFC 2233</p> <p>The LDP implementation supporting the MPLS LDP MIB fully complies with the provisions of Section 10 of RFC 2026, which, in effect, states that the implementation of LDP is recommended for network devices that perform MPLS forwarding along normally routed paths, as determined by destination-based routing protocols.</p>	<i>Interfaces MIB</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **context**
- **show mpls ldp neighbor**
- **snmp mib community-map**
- **snmp mib target list**
- **snmp-server community**
- **snmp-server context**
- **snmp-server enable traps (MPLS)**
- **snmp-server group**
- **snmp-server host**
- **snmp-server trap authentication vrf**

# Glossary

**ATM**—Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.

**downstream-on-demand distribution**—A label distribution method in which a downstream label switch router (LSR) sends a binding upstream only if the upstream LSR requests it.

**downstream unsolicited distribution**—A label distribution method in which labels are dispersed if a downstream label switch router (LSR) needs to establish a new binding with its neighboring upstream LSR. For example, an edge LSR might enable a new interface with another subnet. The LSR then announces to the upstream router a binding to reach this network.

**informs**—A type of notification message that is more reliable than a conventional trap notification message, because the informs message notification requires acknowledgment, but a trap notification does not.

**label**—A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

**label distribution**—The techniques and processes that are used by label switch routers (LSRs) to exchange label binding information for supporting hop-by-hop forwarding along normally routed paths.

**LDP**—Label Distribution Protocol. The protocol that supports MPLS hop-by-hop forwarding and the distribution of bindings between labels and network prefixes. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label-switched path. A configured connection between two label switch routers (LSRs) in which label-switching techniques are used for packet forwarding; also a specific path through an MPLS network.

**LSR**—label switch router. A Multiprotocol Label Switching (MPLS) node that can forward native Layer 3 packets. The LSR forwards a packet based on the value of a label attached to the packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by the use of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A switching method for the forwarding of IP traffic through the use of a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**MPLS label distribution**—A constraint-based routing algorithm for routing label-switched path (LSP) tunnels.

**NMS**—network management station. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks. In the context of SNMP, an NMS is a device that performs SNMP queries to the SNMP agent of a managed device to retrieve or modify information.

**notification**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal to indicate that a significant network event has occurred. *See also* trap.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature of the packet streams they want to receive by specifying such items as bandwidth, jitter, and maximum burst.

**RTR**—Response Time Reporter. A tool that allows you to monitor network performance, network resources, and applications by measuring response times and availability.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP enables a user to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**SNMP communities**—Authentication scheme that enables an intelligent network device to validate SNMP requests.

**SNMPv2c**—Version 2c of the Simple Network Management Protocol. SNMPv2c supports centralized as well as distributed network management strategies and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security.

**SNMPv3**—Version 3 of the Simple Network Management Protocol. Interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting packets over the network.

**TDP**—Tag Distribution Protocol. A standard protocol used by MPLS-enabled routers to negotiate the tags (addresses) used for forwarding packets. *See also* LDP.

**TLV**—Type-Length-Value. A mechanism used by several routing protocols to carry a variety of attributes. Cisco Discovery Protocol (CDP), Label Discovery Protocol (LDP), and Border Gateway Protocol (BGP) are examples of protocols that use TLVs. BGP uses TLVs to carry attributes such as Network Layer Reachability Information (NLRI), Multiple Exit Discriminator (MED), and local preference.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant network event has occurred. Traps (notifications) are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received. *See also* notification.

**VCC**—virtual channel connection. A logical circuit, made up of virtual channel links (VCLs), that carries data between two endpoints in an ATM network. Sometimes called a *virtual circuit connection*.

**VCI**—virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the virtual path identifier (VPI), is used to identify the next network virtual channel link (VCL) as the cell passes through a series of ATM switches on its way to its final destination.

**VCL**—virtual channel link. The logical connection that exists between two adjacent switches in an ATM network.

**VPI**—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the virtual channel identifier (VCI), is used to identify the next network virtual channel link (VCL) as the cell passes through a series of ATM switches on its way to its final destination.

**VPN**—Virtual Private Network. A network that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

**VRF**—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.



# MPLS Traffic Engineering MIB

---

**First Published: May 22, 2001**

**Last Updated: February 18, 2009**

The MPLS Traffic Engineering MIB enables Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) traffic engineering (TE) management, as implemented in the MPLS Traffic Engineering MIB (MPLS TE MIB). The SNMP agent code operating in conjunction with the MPLS TE MIB enables a standardized, SNMP-based approach to be used in managing the MPLS TE features in Cisco IOS software.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for the MPLS Traffic Engineering MIB”](#) section on page 16.

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

## Contents

- [Restrictions for the MPLS Traffic Engineering MIB, page 2](#)
- [Information About the MPLS Traffic Engineering MIB, page 2](#)
- [How to Configure the MPLS Traffic Engineering MIB, page 10](#)
- [Configuration Examples for the MPLS Traffic Engineering MIB, page 13](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)
- [Feature Information for the MPLS Traffic Engineering MIB, page 16](#)
- [Glossary, page 17](#)



---

**Americas Headquarters:**

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

© 2001—2009 Cisco Systems, Inc. All rights reserved.

# Restrictions for the MPLS Traffic Engineering MIB

The following restrictions apply to the MPLS TE MIB for Cisco IOS releases:

- Supports read-only (RO) permission for MIB objects.
- Contains no configuration support by means of SET functions, except for the `mplsTunnelTrapEnable` object (which has been made writable). Accordingly, the MPLS TE MIB contains indexing support for the Interfaces MIB.
- Supports only SNMP GET, GETNEXT, and GETBULK retrieval functions, except in the case of the `mplsTunnelTrapEnable` object (which has been made writable by means of SET functions).
- Contains no support for Guaranteed Bandwidth Traffic Engineering (GBTE) or Auto Bandwidth features.

## Information About the MPLS Traffic Engineering MIB

This section describes the following:

- [MPLS Traffic Engineering MIB Cisco Implementation, page 2](#)
- [Capabilities Supported by the MPLS Traffic Engineering MIB, page 3](#)
- [Notification Generation Events, page 3](#)
- [Notification Implementation, page 4](#)
- [Benefits of MPLS Traffic Engineering MIB, page 4](#)
- [MPLS Traffic Engineering MIB Layer Structure, page 4](#)
- [Features and Technologies Related to MPLS Traffic Engineering MIB, page 5](#)
- [Supported Objects in the MPLS Traffic Engineering MIB, page 5](#)
- [CLI Access to MPLS Traffic Engineering MIB Information, page 9](#)

## MPLS Traffic Engineering MIB Cisco Implementation

The MPLS TE MIB is based on the Internet Engineering Task Force (IETF) draft MIB entitled *draft-ietf-mpls-te-mib-05.txt* which includes objects describing features that support MPLS TE.

Slight differences between the IETF draft MIB and the implementation of the TE capabilities within Cisco IOS software require some minor translations between the MPLS TE MIB and the internal data structures of Cisco IOS software. These translations are made by the SNMP agent code that is installed and operating on various hosts within the network. This SNMP agent code, running in the background as a low priority process, provides a management interface to Cisco IOS software.

The SNMP objects defined in the MPLS TE MIB can be displayed by any standard SNMP utility. All MPLS TE MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS TE MIB.

## MPLS Traffic Engineering Overview

MPLS TE capabilities in Cisco IOS software enable an MPLS backbone to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks.

TE capabilities are essential to effective management of service provider and Internet service provider (ISP) backbones. Such backbones must support high transmission capacities, and the networks incorporating backbones must be extremely resilient to link or node failures.

The MPLS TE facilities built into Cisco IOS software provide a feature-rich, integrated approach to managing the large volumes of traffic that typically flow through WANs. The MPLS TE facilities are integrated into Layer 3 network services, thereby optimizing the routing of IP traffic in the face of constraints imposed by existing backbone transmission capacities and network topologies.

## Capabilities Supported by the MPLS Traffic Engineering MIB

The following functionality is supported in the MPLS Traffic Engineering MIB:

- The ability to generate and queue notification messages that signal changes in the operational status of MPLS TE tunnels.
- Extensions to existing SNMP commands that provide the ability to enable, disable, and configure notification messages for MPLS TE tunnels.
- The ability to specify the name or the IP address of a network management station (NMS) in the operating environment to which notification messages are to be sent.
- The ability to write notification configurations into nonvolatile memory.

## Notification Generation Events

When MPLS TE notifications are enabled (see the **snmp-server enable traps mpls traffic-eng** command), notification messages relating to specific events within Cisco IOS software are generated and sent to a specified NMS in the network.

For example, an `mplsTunnelUp` notification is sent to an NMS when an MPLS TE tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.

Conversely, an `mplsTunnelDown` notification is generated and sent to an NMS when an MPLS TE tunnel transitions from an operationally “up” state to a “down” state.

An `mplstunnelRerouted` notification is sent to the NMS under the following conditions:

- The signaling path of an existing MPLS TE tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).
- The signaling path of an existing MPLS TE tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by:
  - A timer
  - The issuance of an **mpls traffic-eng reoptimize** command
  - A configuration change that requires the resignaling of a tunnel

The `mplsTunnelReoptimized` notification is not generated when an MPLS traffic engineering tunnel is reoptimized. However, an `mplsTunnelReroute` notification is generated. Thus, at the NMS, you cannot distinguish between a tunnel reoptimization event and tunnel reroute event.



Path options are configurable parameters that you can use to specify the order of priority for establishing a new tunnel path. For example, you can create a tunnel head configuration and define any one of many path options numbered 1 through  $n$ , with “1” being the highest priority option and “ $n$ ” being an unlimited number of lower priority path options. Thus, there is no limit to the number of path options that you can specify in this manner.

## Notification Implementation

When an MPLS TE tunnel interface (or any other device interface, such as an Ethernet or Packet over SONET (POS) interface) transitions between an up and down state, an Interfaces MIB (ifMIB) link notification is generated. When such a notification occurs in an MPLS TE MIB environment, the interface is checked by software to determine if the notification is associated with an MPLS TE tunnel. If so, the interfaces MIB link notification is interlinked with the appropriate `mplsTunnelUp` or `mplsTunnelDown` notification to provide notification to the NMS regarding the operational event occurring on the tunnel interface. Hence, the generation of an Interfaces MIB link notification pertaining to an MPLS traffic engineering tunnel interface begets an appropriate `mplsTunnelUp` or `mplsTunnelDown` notification that is transmitted to the specified NMS.

An `mplsTunnelRerouted` notification is generated whenever the signaling path for an MPLS TE tunnel changes. However, software intelligence in the MPLS TE MIB prevents the reroute notification from being sent to the NMS when a TE tunnel transitions between an up or down state during an administrative or operational status check of the tunnel. Either an up or down notification or a reroute notification can be sent in this instance, but not both. This action prevents unnecessary traffic on the network.

## Benefits of MPLS Traffic Engineering MIB

The MPLS Traffic Engineering MIB provides the following benefits:

- Provides a standards-based SNMP interface for retrieving information about MPLS TE.
- Provides information about the traffic flows on MPLS TE tunnels.
- Presents MPLS TE tunnel routes, including the configured route, the Interior Gateway Protocol (IGP) calculated route, and the actual route traversed.
- Provides information, in conjunction with the Interfaces MIB, about how a tunnel was rerouted in the event of a link failure.
- Provides information about the configured resources used for an MPLS TE tunnel.
- Supports the generation and queueing of notifications that call attention to major changes in the operational status of MPLS TE tunnels;
- Forwards notification messages to a designated NMS for evaluation or action by network administrators.

## MPLS Traffic Engineering MIB Layer Structure

The SNMP agent code supporting the MPLS TE MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure similar to that of the MIB support code in Cisco IOS software, consists of four layers:

- Platform independent layer—This layer is generated primarily by the Cisco IOS MIB development tool set and incorporates platform and implementation independent functions. The Cisco IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the Cisco IOS MIB development tool set.
- Application specific layer—This layer provides an interface between the application interface layer and the application program interface (API) and data structures layer and performs tasks needed to retrieve required information from Cisco IOS software, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within Cisco IOS software that are retrieved or called in order to set or retrieve SNMP management information.

## Features and Technologies Related to MPLS Traffic Engineering MIB

The MPLS TE MIB feature is used in conjunction with the following features and technologies:

- Standards-based SNMP network management application
- MPLS
- MPLS TE
- MPLS label switching router MIB (MPLS-LSR-MIB)

## Supported Objects in the MPLS Traffic Engineering MIB

The MPLS TE MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS TE features in Cisco IOS software. The MPLS TE MIB conforms to Abstract Syntax Notation One (ASN.1), thus reflecting an idealized MPLS TE database.

Using any standard SNMP network management application, you can retrieve and display information from the MPLS TE MIB by using GET operations; similarly, you can traverse information in the MIB database for display by using GETNEXT operations.

The MPLS TE MIB tables and objects supported in Cisco IOS releases follow. Important MIB tables (those highlighted in bold type) are described briefly in accompanying text.

- **mplsTunnelConfigured**—Total number of tunnel configurations that are defined on this node.
- **mplsTunnelActive**—Total number of label switched paths (LSPs) that are defined on this node.
- **mplsTunnelTEDistProto**—The IGP distribution protocol in use.
- **mplsTunnelMaxHops**—The maximum number of hops any given tunnel can utilize.
- **mplsTunnelIndexNext**—Unsupported; set to 0.
- **mplsTunnelTable**—Entries in this table with an instance of 0 and a source address of 0 represent tunnel head configurations. All other entries in this table represent instances of LSPs, both signaled and standby. If a tunnel instance is signaled, its operating status (operStatus) is set to “up” (1) and its instance corresponds to an active LSP.

Tunnel configurations exist only on the tunnel head where the tunnel interface is defined. LSPs traverse the network and involve tunnel heads, tunnel midpoints, and tunnel tails.

Pointers in the tunnel table refer to corresponding entries in other MIB tables. By using these pointers, you can find an entry in the `mplsTunnelTable` and follow a pointer to other tables for additional information. The pointers are the following: *mplsTunnelResourcePointer*, *mplsTunnelHopTableIndex*, *mplsTunnelARHopTableIndex*, and *mplsTunnelCHopTableIndex*.

The tunnel table is indexed by tunnel ID, tunnel instance, tunnel source address, and tunnel destination address. The description of each entry has an alphabetic suffix (a), (b), or (c), if appropriate, to indicate the applicability of the entry:

- a. For tunnel head configurations only
- b. For LSPs only
- c. For both tunnel head configurations and LSPs

Following is a list and description of each entry.

- `mplsTunnelIndex`—Same as tunnel ID (c).
- `mplsTunnelInstance`—Tunnel instance of the LSP; 0 for head configurations (b).
- `mplsTunnelIngressLSRId`—Source IP address of the LSP; 0 for head configurations (b).
- `mplsTunnelEgressLSRId`—Destination IP address of the tunnel (c).
- `mplsTunnelName`—Command name for the tunnel interfaces (a).
- `mplsTunnelDescr`—Descriptive name for tunnel configurations and LSPs (c).
- `mplsTunnelIsIf`—Indicator of whether the entry represents an interface (c).
- `mplsTunnelIfIndex`—Index of the tunnel interface within the `ifMIB` (a).
- `mplsTunnelXCPointer`—(For midpoints only – no tails) Pointer for the LSP within the `mplsXCTable` of the MPLS LSR MIB (b).
- `mplsTunnelSignallingProto`—Signaling protocol used by tunnels (c).
- `mplsTunnelSetupPrio`—Setup priority of the tunnel (c).
- `mplsTunnelHoldingPrio`—Holding priority of the tunnel (c).
- `mplsTunnelSessionAttributes`—Session attributes (c).
- `mplsTunnelOwner`—Tunnel owner (c).
- `mplsTunnelLocalProtectInUse`—Not implemented (c).
- `mplsTunnelResourcePointer`—Pointer into the Resource Table (b).
- `mplsTunnelInstancePriority`—Not implemented (b).
- `mplsTunnelHopTableIndex`—Index into the Hop Table (a).
- `mplsTunnelARHopTableIndex`—Index into the AR Hop Table (b).
- `mplsTunnelCHopTableIndex`—Index into the C Hop Table (b).
- `mplsTunnelPrimaryTimeUp`—Amount of time, in seconds, that the current path has been up (a).
- `mplsTunnelPathChanges`—Number of times a tunnel has been ressignaled (a).
- `mplsTunnelLastPathChange`—Amount of time, in seconds, since the last path ressignaling occurred (a).
- `mplsTunnelCreationTime`—Time stamp when the tunnel was created (a).
- `mplsTunnelStateTransitions`—Number of times the tunnel has changed state (a).
- `mplsTunnelIncludeAnyAffinity`—Not implemented (a).

- `mplsTunnelIncludeAllAffinity`—Attribute bits that must be set for the tunnel to traverse a link (a).
- `mplsTunnelExcludeAllAffinity`—Attribute bits that must *not* be set for the tunnel to traverse a link (a).
- `mplsTunnelPathInUse`—Path option number being used for the tunnel’s path. If no path option is active, this object will be 0 (a).
- `mplsTunnelRole`—Role of the tunnel on the router; that is, head, midpoint, or tail (c).
- `mplsTunnelTotalUptime`—Amount of time, in seconds, that the tunnel has been operationally up (a).
- `mplsTunnelInstanceUptime`—Not implemented (b).
- `mplsTunnelAdminStatus`—Administrative status of a tunnel (c).
- `mplsTunnelOperStatus`—Actual operating status of a tunnel (c).
- `mplsTunnelRowStatus`—This object is used in conjunction with configuring a new tunnel. This object will always be seen as “active” (a).
- `mplsTunnelStorageType`—Storage type of a tunnel entry (c).
- `mplsTunnelHopListIndexNext`—Next valid index to use as an index in the `mplsTunnelHopTable`.
- **`mplsTunnelHopTable`**—Entries in this table exist only for tunnel configurations and correspond to the path options defined for the tunnel. Two types of path options exist: *explicit* and *dynamic*. This table shows all hops listed in the explicit path options, while showing only the destination hop for dynamic path options. The tunnel hop table is indexed by tunnel ID, path option, and hop number.

Following is a list and description of each table entry.

- `mplsTunnelHopListIndex`—Primary index into the table.
- `mplsTunnelHopIndex`—Secondary index into the table.
- `mplsTunnelHopAddrType`—Indicates if the address of this hop is the type IPv4 or IPv6.
- `mplsTunnelHopIpv4Addr`—The IPv4 address of this hop.
- `mplsTunnelHopIpv4PrefixLen`—The prefix length of the IPv4 address.
- `mplsTunnelHopIpv6Addr`—The IPv6 address of this hop.
- `mplsTunnelHopIpv6PrefixLen`—The prefix length of the IPv6 address.
- `mplsTunnelHopAsNumber`—This object will contain 0 or the autonomous system number of the hop, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopLspId`—This object will contain 0 or the LSPID of the tunnel, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopType`—Denotes whether this tunnel hop is routed in a strict or loose fashion.
- `mplsTunnelHopRowStatus`—This object is used in conjunction with the configuring of a new row in the table.
- `mplsTunnelHopStorageType`—The storage type of this MIB object.
- `mplsTunnelResourceIndexNext`—This object contains the next appropriate value to be used for `mplsTunnelResourceIndex` when creating entries in the `mplsTunnelResourceTable`.
- **`mplsTunnelResourceTable`**—Entries in this table correspond to the “Tspec” information displayed when you execute the **`show mpls traffic-eng tunnels`** command. These entries exist only for LSPs.

The tunnel resource table is indexed by address and hop number. Following the *mplsTunnelResourcePointer* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry.

- *mplsTunnelResourceIndex*—The primary index into this table.
- *mplsTunnelResourceMaxRate*—The maximum rate, in bits per second, supported by this tunnel.
- *mplsTunnelResourceMeanRate*—The mean rate, in bits per second, supported by this tunnel.
- *mplsTunnelResourceMaxBurstSize*—The maximum burst size, in bytes, allowed by this tunnel.
- *mplsTunnelResourceRowStatus*—This object is used in conjunction with the configuration of a new row in the table.
- *mplsTunnelResourceStorageType*—The storage type of this MIB object.
- **mplsTunnelARHopTable**—Entries in this table correspond to the actual route taken by the tunnel, and whose route was successfully signaled by the network. The hops present in this table correspond to those present in the record route object (RRO) in Resource Reservation Protocol (RSVP). You can also display the information in this table by executing the **show mpls traffic-eng tunnels** command.

The actual route hop table is indexed by address and hop number. Following the *mplsTunnelARHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry:

- *mplsTunnelARHopListIndex*—The primary index into this table.
- *mplsTunnelARHopIndex*—The secondary index into this table.
- *mplsTunnelARHopIpv4Addr*—The IPv4 address of this hop.
- *mplsTunnelARHopIpv4PrefixLen*—The prefix length of the IPv4 address.
- *mplsTunnelARHopIpv6Addr*—The IPv6 address of this hop.
- *mplsTunnelARHopIpv6PrefixLen*—The prefix length of the IPv6 address.
- *mplsTunnelARHopAsNumber*—This object will contain 0 or the AS number of the hop, depending on the value of *mplsTunnelARHopAddrType*.
- *mplsTunnelARHopAddrType*—The type of address for this MIB entry, either IPv4 or IPv6.
- *mplsTunnelARHopType*—Denotes whether this tunnel hop is routed in a strict or loose manner.
- **mplsTunnelCHopTable**—Entries in this table correspond to the explicit route object (ERO) in RSVP, which is used to signal the LSP. The list of hops in this table will contain those hops that are computed by the constraint-based shortest path first (SPF) algorithm. In those cases where “loose” hops are specified for the tunnel, this table will contain the hops that are “filled-in” between the loose hops to complete the path. If you specify a complete explicit path, the computed hop table matches your specified path.

The computed hop table is indexed by address and hop number. Following the *mplsTunnelCHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry:

- *mplsTunnelCHopListIndex*—The primary index into this table.
- *mplsTunnelCHopIndex*—The secondary index into this table.
- *mplsTunnelCHopAddrType*—Indicates if the address of this hop is the type IPv4 or IPv6.

- `mplsTunnelCHopIpv4Addr`—The IPv4 address of this hop.
- `mplsTunnelCHopIpv4PrefixLen`—The prefix length of the IPv4 address.
- `mplsTunnelCHopIpv6Addr`—The IPv6 address of this hop.
- `mplsTunnelCHopIpv6PrefixLen`—The prefix length of the IPv6 address.
- `mplsTunnelCHopAsNumber`—This object will contain 0 or the autonomous system number of the hop, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelCHopType`—Denotes whether this tunnel hop is routed in a strict or loose way.
- **`mplsTunnelPerfTable`**—The tunnel performance table, which augments the **`mplsTunnelTable`**, provides packet and byte counters for each tunnel. This table contains the following packet and byte counters:
  - `mplsTunnelPerfPackets`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfHCPackets`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfErrors`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfBytes`—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.
  - `mplsTunnelPerfHCBytes`—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.
- `mplsTunnelTrapEnable`—The object type *mplsTunnelTrapEnable* is enhanced to be writable. Accordingly, if this object type is set to “TRUE,” the following notifications are enabled, thus giving you the ability to monitor changes in the operational status of MPLS TE tunnels:
  - `mplsTunnelUp`
  - `mplsTunnelDown`
  - `mplsTunnelRerouted`

If the *mplsTunnelTrapEnable* object is set to “FALSE,” such operational status notifications are not generated. These notification functions are based on the definitions (`mplsTeNotifications`) contained in the IETF draft document entitled *draft-ietf-mpls-te-mib-05.txt*.

## CLI Access to MPLS Traffic Engineering MIB Information

Figure 1 shows commands that you can use to retrieve information from specific tables in the MPLS TE MIB. As noted in this figure, some information in the MPLS TE MIB is not retrievable by commands.

**Figure 1**      **Commands for Retrieving MPLS TE MIB Information**

		show mpls traffic-eng tunnels	show mpls traffic-eng summary	show ip explicit-paths	show interfaces	Not available in command
mplsTunnelTable	x				x	
mplsTunnelHopTable	x		x			
mplsTunnelResourceTable	x					
mplsTunnelARHopTable	x					
mplsTunnelCHopTable	x					
mplsTunnelPerfTable	x			x		
Scalars	x	x			x	

52510

## Retrieving Information from the MPLS Traffic Engineering MIB

This section describes how to efficiently retrieve information about TE tunnels. Such information can be useful in large networks that contain many TE tunnels.

Traverse across a single column of the *mplsTunnelTable*, such as *mplsTunnelName*. This action provides the indexes of every tunnel configuration, and any LSPs involving the host router. Using these indexes, you can perform a GET operation to retrieve information from any column and row of the *mplsTunnelTable*.

The *mplsTunnelTable* provides pointers to other tables for each tunnel. The column *mplsTunnelResourcePointer*, for example, provides an object ID (OID) that you can use to access resource allocation information in the *mplsTunnelResourceTable*. The columns *mplsTunnelHopTableIndex*, *mplsTunnelARHopTableIndex*, and *mplsTunnelCHopTableIndex* provide the primary index into the *mplsTunnelHopTable*, *mplsTunnelARHopTable*, and *mplsTunnelCHopTable*, respectively. By traversing the MPLS TE MIB in this manner using a hop table column and primary index, you can retrieve information pertaining to the hops of that tunnel configuration.

Because tunnels are treated as interfaces, the tunnel table column (*mplsTunnelIfIndex*) provides an index into the Interfaces MIB that you can use to retrieve interface-specific information about a tunnel.

## How to Configure the MPLS Traffic Engineering MIB

This section contains the following tasks:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router, page 11](#) (required)

- [Verifying the Status of the SNMP Agent, page 12](#) (optional)

## Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router

The SNMP agent for the MPLS TE MIB is disabled by default. To enable the SNMP agent for the MPLS TE MIB, perform the following steps.

### SUMMARY STEPS

1. `telnet host`
2. `enable`
3. `show running-config`
4. `configure terminal`
5. `snmp-server community string [view view-name] [ro | rw] [ipv6 nacl] [access-list-number]`
6. `snmp-server enable traps [identification-type] [notification-option]`
7. `exit`
8. `write memory`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>telnet host</code>  <b>Example:</b> Router> telnet 192.172.172.172	Telnets to the router identified by the specified IP address (represented as xxx.xxx.xxx.xxx).
Step 2	<code>enable</code>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 3	<code>show running-config</code>  <b>Example:</b> Router# show running-config	Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"> <li>• If no SNMP information is displayed, go to <a href="#">Step 4</a>. If any SNMP information is displayed, you can modify the information or change it as needed.</li> </ul>
Step 4	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.



	Command or Action	Purpose
<b>Step 5</b>	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <b>ipv6</b> <i>nacl</i> ] [ <i>access-list-number</i> ]  <b>Example:</b> Router(config)# snmp-server community comaccess ro 4	Enables the read-only (RO) community string.
<b>Step 6</b>	<b>snmp-server enable traps</b> [ <i>identification-type</i> ] [ <i>notification-option</i> ]  <b>Example:</b> Router(config)# snmp-server enable traps	Enables an LSR to send SNMP notifications or informs to an SNMP host.  <b>Note</b> This command is optional. After SNMP is enabled, all MIBs (not just the TE MIB) are available for the user to query.
<b>Step 7</b>	<b>exit</b>  <b>Example:</b> Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.
<b>Step 8</b>	<b>write memory</b>  <b>Example:</b> Router# write memory	Writes the modified configuration to NVRAM, permanently saving the settings.

## Verifying the Status of the SNMP Agent

To verify that the SNMP agent has been enabled on a host network device, perform the following steps.

### SUMMARY STEPS

1. **telnet** *host*
2. **enable**
3. **show running-config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>telnet</b> <i>host</i>  <b>Example:</b> Router# telnet 192.172.172.172	Telnet to the target device identified by the specified IP address (represented as <i>xxx.xxx.xxx.xxx</i> ).
Step 2	<b>enable</b>  <b>Example:</b> Router# enable	Enables SNMP on the target device.
Step 3	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration on the target device and is used to examine the output for displayed SNMP information.

## Examples

The following example displays the running configuration on the target device and its SNMP information.

```
Router# show running-config
.
.
.
snmp-server community public ro
snmp-server community private ro
```

Any **snmp-server** statement that appears in the output and takes the form shown here verifies that SNMP has been enabled on that device.

## Configuration Examples for the MPLS Traffic Engineering MIB

This section contains the following configuration examples:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example, page 13](#)

### Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example

The following example shows how to enable an SNMP agent on a host network device:

```
Router# configure terminal
Router(config)# snmp-server community private
```

The following example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP agent to access all MPLS TE MIB objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

The following example shows how to allow read-only access to all MPLS TE MIB objects relating to members of access list 4 that specify the *comaccess* community string. No other SNMP agents will have access to any MPLS TE MIB objects.

```
Router(config)# snmp-server community comaccess ro 4
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering MIB.

### Related Documents

Related Topic	Document Title
MPLS-based functionalities	<ul style="list-style-type: none"> <li><i>MPLS Label Distribution Protocol (LDP)</i></li> <li><i>MPLS Label Switching Router MIB</i></li> <li><i>MPLS Scalability Enhancements for the LSC LSR</i></li> <li><i>MPLS Scalability Enhancements for the ATM LSR</i></li> <li><i>MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for MPLS TE Tunnels</i></li> <li><i>MPLS Traffic Engineering (TE)—Scalability Enhancements</i></li> <li><i>MPLS Class of Service Enhancements</i></li> <li><i>RFC 2233 Interfaces MIB</i></li> </ul>

### Standards

Standard	Title
draft-ietf-mpls-te-mib-05	MPLS Traffic Engineering Management Information Base Using SMIv2

### MIBs

MIB	MIBs Link
MPLS TE MIB Interfaces MIB	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 2026	<i>The Internet Standards Process</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- **snmp-server community**
- **snmp-server enable traps mpls traffic-eng**
- **snmp-server host**

# Feature Information for the MPLS Traffic Engineering MIB

Table 1 lists the release history for this MIB.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for the MPLS Traffic Engineering MIB

Feature Name	Releases	Feature Information
MPLS Traffic Engineering MIB	12.0(17)S 12.0(17)ST 12.2(8)T 12.2(14)S 12.2(28)SB 12.2(31)SB2	<p>The MPLS Traffic Engineering MIB feature enables the SNMP agent support in Cisco IOS software for MPLS TE management, as implemented in the MPLS TE MIB.</p> <p>In 12.0(17)S, this feature provided the ability to generate and queue SNMP notification messages that signal changes in the operational status of MPLS TE tunnels when you are using the MPLS TE MIB on Cisco 7500 series routers and Cisco 12000 series Internet routers.</p> <p>In 12.0(17)ST, support for SNMP traffic engineering notifications was extended to include Cisco 7500 series routers and Cisco 12000 series Internet routers.</p> <p>In 12.2(8)T, support for SNMP TE notifications was extended to include Cisco 7500 series routers. The <b>snmp-server host</b> command was modified.</p> <p>In 12.2(14)S, this feature was integrated.</p> <p>In 12.2(28)SB, this feature was integrated.</p> <p>In 12.2(31)SB2, this feature was integrated.</p> <p>The following commands were introduced or modified: <b>snmp-server community</b>, <b>snmp-server enable traps mpls traffic-eng</b>, <b>snmp-server host</b>.</p>

# Glossary

**affinity bits**—An MPLS traffic engineering tunnel’s requirements on the attributes of the links it will cross. The tunnel’s affinity bits and affinity mask must match with the attributes of the various links carrying the tunnel.

**call admission precedence**—An MPLS traffic engineering tunnel with a higher priority will, if necessary, preempt an MPLS traffic engineering tunnel with a lower priority. An expected use is that tunnels that are more difficult to route will have a higher priority, and can preempt tunnels that are less difficult to route, on the assumption that those lower priority tunnels can find another path.

**constraint-based routing**—Procedures and protocols used to determine a route across a backbone taking into account resource requirements and resource availability, instead of simply using the shortest path.

**flow**—A traffic load entering the backbone at one point—point of presence (POP)—and leaving it from another that must be traffic engineered across the backbone. The traffic load will be carried across one or more LSP tunnels running from the entry POP to the exit POP.

**headend**—The LSR at which the tunnel originates. The tunnel’s “head” or tunnel interface will reside at this LSR as well.

**informs**—A type of notification message that is more reliable than a conventional trap notification message because an informs message requires acknowledgment.

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**label switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**LSP**—label switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MIB**—Management Information Base. A database of network management information (consisting of MIB objects) that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually by a GUI-based network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**NMS**—network management station. An NMS is a powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**notification**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred (see traps).

**OSPF**—Open Shortest Path First. A link-state routing protocol used for routing IP.

**RSVP**—Resource Reservation Protocol. Protocol for reserving network resources to provide quality of service (QoS) guarantees to application flows.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**tailend**—The downstream, receive end of a tunnel.

**traffic engineering**—Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred. Traps (notifications) are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received (see notification).

**VCC**—virtual channel connection. A VCC is a logical circuit consisting of VCLs that carries data between two endpoints in an ATM network. Sometimes called a virtual circuit connection.

**VCI**—virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next network VCL as the cell passes through a series of ATM switches on its way to its final destination.

**VCL**—virtual channel link. A VCL is the logical connection that exists between two adjacent switches in an ATM network.

**VPI**—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next network VCL as the cell passes through a series of ATM switches on its way to its final destination.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2001—2009 Cisco Systems, Inc. All rights reserved.



# MPLS Traffic Engineering—Fast Reroute MIB

---

**First Published: March 30, 2001**

**Last Updated: February 27, 2009**

The MPLS Traffic Engineering—Fast Reroute MIB provides Simple Network Management Protocol (SNMP)-based network management of the Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) feature in Cisco IOS software.

The Fast Reroute MIB has the following features:

- Notifications can be created and queued.
- Command-line interface (CLI) commands enable notifications, and specify the IP address to where the notifications will be sent.
- The configuration of the notifications can be written into nonvolatile memory.

The MIB includes objects describing features within MPLS FRR, and it includes the following tables:

- cmplsFrrConstTable
- cmplsFrrLogTable
- cmplsFrrFacRouteDBTable

The MIB also includes scalar objects (that is, objects that are not in a table). For more information, see the [“FRR MIB Scalar Objects” section on page 4](#).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS Traffic Engineering—Fast Reroute MIB” section on page 17](#).

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



---

**Americas Headquarters:**

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



# Contents

- [Prerequisites for the MPLS Traffic Engineering—Fast Reroute MIB, page 2](#)
- [Restrictions for the MPLS Traffic Engineering—Fast Reroute MIB, page 3](#)
- [Information About the MPLS Traffic Engineering—Fast Reroute MIB, page 3](#)
- [How to Configure the MPLS Traffic Engineering—Fast Reroute MIB, page 8](#)
- [Configuration Examples for the MPLS Traffic Engineering—Fast Reroute MIB, page 14](#)
- [Additional References, page 15](#)
- [Feature Information for MPLS Traffic Engineering—Fast Reroute MIB, page 17](#)
- [Glossary, page 18](#)

## Prerequisites for the MPLS Traffic Engineering—Fast Reroute MIB

- The network must support the Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF) protocol.
- The SNMP is installed and enabled on the label switch routers (LSRs).
- MPLS is enabled globally on each LSR.
- Cisco Express Forwarding is enabled on the LSRs.
- Traffic engineering (TE) tunnels are enabled.
- MPLS FRR is enabled on one of the TE tunnels.
- The Resource Reservation Protocol (RSVP) is enabled.

## Restrictions for the MPLS Traffic Engineering—Fast Reroute MIB

- The implementation of the FRR MIB is limited to read-only (RO) permission for MIB objects.
- Configuration of the FRR MIB using the SNMP SET command is not supported in Cisco IOS Release 12.2(33)SRA or in prior releases.
- The following tables are not implemented in the specified releases:
  - mplsFrrOne2OnePlrTable—Not implemented in Cisco IOS software.
  - mplsFrrDetourTable—Not implemented in Cisco IOS software.
  - cmplsFrrLogTable—Implemented only in Cisco IOS 12.0S-based releases.

# Information About the MPLS Traffic Engineering—Fast Reroute MIB

To use the MPLS Traffic Engineering—Fast Reroute MIB, you need to understand the following concepts:

- [Feature Design of the MPLS Traffic Engineering—Fast Reroute MIB, page 3](#)
- [Functional Structure of the MPLS Traffic Engineering—Fast Reroute MIB, page 3](#)
- [System Flow of SNMP Protocol Requests and Response Messages, page 4](#)
- [FRR MIB Scalar Objects, page 4](#)
- [FRR MIB Notifications, page 5](#)
- [MIB Tables in the MPLS Traffic Engineering—Fast Reroute MIB, page 6](#)

## Feature Design of the MPLS Traffic Engineering—Fast Reroute MIB

The FRR MIB enables standard, SNMP-based network management of FRR in Cisco IOS software. This capability requires that SNMP agent code executes on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MIB.

The FRR MIB is based on the Internet Engineering Task Force (IETF) draft MIB specification *draft-ietf-mpls-fastreroute-mib-02.txt*. The IETF draft MIB, which undergoes revisions periodically, is evolving toward becoming a standard. The Cisco implementation of the FRR MIB is expected to track the evolution of the IETF draft MIB, and may change accordingly.

Slight differences between the IETF draft MIB and the implementation of FRR within Cisco IOS software require some minor translations between the FRR MIB objects and the internal data structures of Cisco IOS software. These translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low priority process and provides a management interface to Cisco IOS software.

You can use an SNMP agent to access FRR MIB objects using standard SNMP GET operations. All the objects in the FRR MIB follow the conventions defined in the IETF draft MIB.

## Functional Structure of the MPLS Traffic Engineering—Fast Reroute MIB

The SNMP agent code supporting the FRR MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS tool set, based on the MIB source code. The basis for the generated code is the Cisco version of the FRR MIB CISC0-ietf-frr-mib.

The SNMP agent code, which has a layered structure that is common to MIB support code in Cisco IOS software, consists of the following layers:

- **Platform-independent layer**—This layer is generated primarily by the MIB development Cisco IOS tool set and incorporates platform- and implementation-independent functions. These functions handle SNMP standard functionality in the context of the specific MIB. This layer handles indexes and range or enumeration value checks for GET, GET-NEXT, and SET SNMP operations. A function is generated for each SNMP table or group of objects. This layer calls into the next layer.
- **Application interface layer**—The Cisco IOS tool set generates the function names and template code for MIB objects.

- Application-specific layer—This layer provides the mechanism for retrieving relevant data from the managed application layer. It includes an entry point function for each table. This function calls two other functions; one that searches the TE tunnel database that RSVP maintains for the relevant data according to the indexes, and another function that fills the data into the structure.
- Managed application layer—This layer includes all the structures and mechanisms, and is managed by the MIB.

## System Flow of SNMP Protocol Requests and Response Messages

All SNMP protocol requests and response messages are ultimately handled by the SNMP master agent. When such a message is received on a router, the master agent parses the requests and identifies the MIB to which the request refers. The master agent then queries the subagent responsible for the MIB with a GET, GET-NEXT, or SET request. The FRR MIB subagent retrieves the appropriate data, and returns it to the master agent. The master agent is then responsible for returning an SNMP response to the NMS. All queries occur within the IP SNMP Cisco IOS process, which runs as a low priority task.

## FRR MIB Scalar Objects

Scalar objects are objects that are not in tables. A scalar object has one instance (that is, one occurrence).

[Table 1](#) describes the FRR MIB scalar objects.

**Table 1**      *Scalar Objects*

MIB Object	Function
cmplsFrrDetourIncoming	Number of detour link-state packets (LSPs) entering the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrDetourOutgoing	Number of detour LSPs leaving the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrDetourOriginating	Number of detour LSPs originating from the device. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrSwitchover	Number of tunnels that are being backed up because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrNumOfConfIfs	Number of MPLS interfaces FRR configured for protection; 0 indicates that LSPs traversing any interface can be protected.
cmplsFrrActProtectedIfs	Number of interfaces FRR is protecting because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrConfProtectingTuns	Number of backup Fast Reroute-protected tunnels configured because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrActProtectedTuns	Number of tunnels protected by the Fast Reroute feature. This object returns 0 because cmplsFrrConstProtectionMethod is set to facilityBackup(1).
cmplsFrrActProtectedLSPs	Number of LSPs that FRR is protecting. If cmplsFrrConstProtectionMethod is set to facilityBackup(1), this object returns 0.
cmplsFrrConstProtectionMethod	This object always returns facilityBackup(1) because Cisco supports only the facility backup protection method.

**Table 1**      *Scalar Objects (continued)*

MIB Object	Function
cmplsFrrNotifsEnabled	A value that indicates whether FRR notifications defined in this MIB are enabled or disabled. This object returns True(1) for enabled, or False(2) for disabled. The default is that notifications are disabled.
cmplsFrrLogTableMaxEntries	Maximum number of entries allowed in the FRR log table. In Cisco IOS 12.0S-based releases, this object always returns 32.
cmplsFrrLogTableCurrEntries	Current number of entries in the FRR log table. Except in Cisco IOS-based releases, this object always returns 0.
cmplsFrrNotifMaxRate	Maximum interval rate between FRR MIB notifications. This object always returns 0.

## FRR MIB Notifications

Notifications are issued after particular FRR events occur. This section provides the following information about FRR MIB notifications supported in Cisco IOS Release 12.0(26)S and in prior releases, Cisco IOS Release 12.2(33)SRA, Cisco IOS Release 12.2(33)SXH, and Cisco IOS Release 12.4(20)T:

- [Notification Generation Events, page 5](#)
- [Notification Specification, page 5](#)
- [Notification Monitoring, page 6](#)

### Notification Generation Events

When you enable FRR MIB notification functionality by issuing the **snmp-server enable traps mpls fast-reroute** command, FRR events generate notification messages that are sent to a designated NMS in the network to signal the occurrence of specific events in Cisco IOS software.

The FRR MIB objects involved in FRR status transitions and event notifications include cmplsFrrProtected. This message is sent to an NMS if there is a major TE tunnel change (that is, fast rerouting of TE tunnels).

### Notification Specification

Each FRR notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type. The generic type for all FRR notifications is “enterprise Specific” because this is not one of the generic notification types defined for SNMP. The enterprise-specific type is 1 for cmplsFrrProtected.

Each notification contains the following objects from the FRR MIB so that the FRR tunnel can be easily identified:

- cmplsFrrConstNumProtectingTunOnIf
- cmplsFrrConstNumProtectedTunOnIf
- cmplsFrrConstBandwidth

Upon being invoked, the appropriate FRR interface indexes have already been retrieved by existing FRR code. The FRR interfaces are then used to fill in data for the three objects included in the notification.

## Notification Monitoring

When FRR MIB notifications are enabled (see the **snmp-server enable traps** command), notification messages relating to specific FRR events within Cisco IOS software are generated and sent to a specified NMS in the network. Any utility that supports SNMPv1 or SNMPv2 notifications can receive notification messages.

To monitor FRR MIB notifications, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

## MIB Tables in the MPLS Traffic Engineering—Fast Reroute MIB

The FRR MIB consists of the following tables:

- [cmplsFrrConstTable](#), page 6
- [cmplsFrrLogTable](#), page 7
- [cmplsFrrFacRouteDBTable](#), page 7

The tables access various data structures to obtain information regarding detours, the FRR database, and logging.

### cmplsFrrConstTable

cmplsFrrConstTable displays the configuration of an FRR-enabled tunnel and the characteristics of its accompanying backup tunnels. For each protected tunnel, there can be multiple backup tunnels.

The table is indexed by the following:

- cmplsFrrConstIfIndex
- cmplsFrrConstTunnelIndex
- cmplsFrrConstTunnelInstance

[Table 2](#) describes the MIB objects for cmplsFrrConstTable.

**Table 2** *cmplsFrrConstTable Objects*

MIB Object	Function
cmplsFrrConstIfIndex	Uniquely identifies an interface on which FRR is configured. If an index has a value of 0, the configuration applies to all interfaces on the device on which the FRR feature can operate.
cmplsFrrConstTunnelIndex	Tunnel for which FRR is requested.
cmplsFrrConstTunnelInstance	Tunnel for which FRR is requested. The value always is 0 because only tunnel heads are represented, and tunnel heads have an instance value of 0.
cmplsFrrConstSetupPrio	Setup priority of the backup tunnel.
cmplsFrrConstHoldingPrio	Holding priority of the backup tunnel.
cmplsFrrConstInclAnyAffinity	Attribute bits that must be set for the tunnel to traverse a link.
cmplsFrrConstInclAllAffinity	Attribute bits that must not be set for the tunnel to traverse a link.
cmplsFrrConstExclAllAffinity	A link satisfies the exclude-all constraint only if the link contains none of the administrative groups specified in the constraint.

**Table 2** *cmplsFrrConstTable Objects (continued)*

MIB Object	Function
cmplsFrrConstHopLimit	The maximum number of hops that the backup tunnel can traverse.
cmplsFrrConstBandwidth	The bandwidth of the backup tunnels for this tunnel, in thousands of bits per second (kbps).
cmplsFrrConstRowStatus	Creates, modifies, and deletes a row in this table.

## cmplsFrrLogTable



### Note

cmplsFrrLogTable and the **show mpls traffic-eng fast-reroute log reroutes** command are supported only in Cisco IOS 12.0S-based releases.

cmplsFrrLogTable is indexed by the object cmplsFrrLogIndex. The index corresponds to a log entry in the FRR feature's **show mpls traffic-eng fast-reroute log reroutes** command. That **show** command stores up to 32 entries at a time. If entries are added, the oldest entry is overwritten with new log information.

cmplsFrrLogTable can store up to 32 entries at a time, overwriting older entries as newer ones are added. The index cmplsFrrLogIndex is incremented to give each log table entry of the MIB a unique index value. Therefore, it is possible to have indexes greater than 32 even though only 32 entries are displaying.

[Table 3](#) describes the MIB objects for cmplsFrrLogTable.

**Table 3** *cmplsFrrLogTable Objects*

MIB Object	Function
cmplsFrrLogIndex	Number of the FRR event.
cmplsFrrLogEventTime	Number of milliseconds that elapsed from bootstrap time to the time that the event occurred.
cmplsFrrLogInterface	Identifies the interface that was affected by this FRR event. The value can be set to 0 if mplsFrrConstProtectionMethod is set to oneToOneBackup(0).
cmplsFrrLogEventType	The type of FRR event that occurred. The object returns Protected or Other.
cmplsFrrLogEventDuration	Duration of the event, in milliseconds.
cmplsFrrLogEventReasonString	Implementation-specific explanation of the event. The object returns interface down event or interface other event.

## cmplsFrrFacRouteDBTable

The following indexes specify which interface and tunnel are being protected by the FRR feature:

- cmplsFrrFacRouteProtectedIfIndex
- cmplsFrrFacRouteProtectedTunIndex

The following indexes specify the backup tunnel that provides protection to the protected tunnel:

- `cmplsFrrFacRouteProtectedIfIndex`
- `cmplsFrrFacRouteProtectingTunIndex`
- `cmplsFrrFacRouteProtectedTunIndex`
- `cmplsFrrFacRouteProtectedTunInstance`
- `cmplsFrrFacRouteProtectedTunIngressLSRId`
- `cmplsFrrFacRouteProtectedTunEgressLSRId`

This version of the MIB will attempt to leverage the work already done for the MPLS TE MIB because it contains similar lookup functions for TE tunnels.

[Table 4](#) describes the MIB objects for `cmplsFrrFacRouteDBTable`.

**Table 4** *cmplsFrrFacRouteDBTable Objects*

MIB Object	Function
<code>cmplsFrrFacRouteProtectedIfIndex</code>	Interface configured for FRR protection.
<code>cmplsFrrFacRouteProtectingTunIndex</code>	The tunnel number of the protecting (backup) tunnel.
<code>cmplsFrrFacRouteProtectedTunIndex</code>	The <code>mplsTunnelEntry</code> primary index for the tunnel head interface designated to protect the interface specified in <code>mplsFrrFacRouteIfProtIdx</code> (and all the tunnels using this interface).
<code>cmplsFrrFacRouteProtectedTunInstance</code>	An <code>mplsTunnelEntry</code> that is being protected by FRR. An instance uniquely identifies a tunnel.
<code>cmplsFrrFacRouteProtectedTunIngressLSRId</code>	Inbound label for the backup LSR.
<code>cmplsFrrFacRouteProtectedTunEgressLSRId</code>	Outbound label for the backup LSR.
<code>cmplsFrrFacRouteProtectedTunStatus</code>	State of the protected tunnel. Valid values are: <ul style="list-style-type: none"> <li>• <code>active</code>—Tunnel label has been placed in the Label Forwarding Information Base (LFIB) and is ready to be applied to incoming packets.</li> <li>• <code>ready</code>—Tunnel's label entry has been created, but is not in the LFIB.</li> <li>• <code>partial</code>—Tunnel's label entry has not been fully created.</li> </ul>
<code>cmplsFrrFacRouteProtectingTunResvBw</code>	Amount of bandwidth, in megabytes per second, that is reserved by the backup tunnel.
<code>cmplsFrrFacRouteProtectingTunProtectionType</code>	Type of protection: 0 designates link protection; 1 designates node protection.

## How to Configure the MPLS Traffic Engineering—Fast Reroute MIB

This section contains the following tasks:

- [Enabling the SNMP Agent for FRR MIB Notifications, page 9](#) (required)
- [Enabling Cisco Express Forwarding, page 10](#) (required)

- [Enabling TE Tunnels, page 11](#) (required)
- [Enabling MPLS FRR on Each TE Tunnel, page 12](#) (required)
- [Enabling a Backup Tunnel on an Interface, page 13](#) (required)

## Enabling the SNMP Agent for FRR MIB Notifications

To enable the SNMP agent for FRR MIB notifications, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community *string* [view *view-name*] [ro] [*access-list-number*]**
5. **snmp-server enable traps mpls fast-reroute protected**
6. **end**
7. **write memory**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration of the router to determine if an SNMP agent is already running on the device.  If no SNMP information is displayed, continue with the next step.  If any SNMP information is displayed, you can modify or change the information.
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>snmp-server community <i>string</i> [view <i>view-name</i>] [ro] [<i>access-list-number</i>]</b>  <b>Example:</b> Router(config)# snmp-server community public ro	Configures read-only (ro) SNMP community strings for the FRR MIB.



	Command or Action	Purpose
Step 5	<b>snmp-server enable traps mpls fast-reroute protected</b>  <b>Example:</b> Router(config)# snmp-server enable traps mpls fast-reroute protected	Enables Fast Reroute traps.
Step 6	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.
Step 7	<b>write memory</b>  <b>Example:</b> Router# write memory	Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.

## Enabling Cisco Express Forwarding

To enable Cisco Express Forwarding, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<code>ip cef distributed</code>  <b>Example:</b> Router(config)# ip cef distributed	Enables distributed Cisco Express Forwarding.
Step 4	<code>end</code>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

## Enabling TE Tunnels

To enable TE tunnels, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip cef`
4. `mpls traffic-eng tunnels`
5. `interface typeslot/port`
6. `mpls traffic-eng tunnels`
7. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>ip cef</code>  <b>Example:</b> Router(config)# ip cef	Enables standard Cisco Express Forwarding operations.
Step 4	<code>mpls traffic-eng tunnels</code>  <b>Example:</b> Router(config)# mpls traffic-eng tunnels	Enables the MPLS TE tunnel feature on a device.

	Command or Action	Purpose
Step 5	<code>interface typeslot/port</code>  <b>Example:</b> Router(config)# interface POS1/0	Specifies the interface and enters interface configuration mode.
Step 6	<code>mpls traffic-eng tunnels</code>  <b>Example:</b> Router(config-if)# mpls traffic-eng tunnels	Enables the MPLS TE tunnel feature on an interface.
Step 7	<code>end</code>  <b>Example:</b> Router(config-if)# end	Returns to privileged EXEC mode.

## Enabling MPLS FRR on Each TE Tunnel

To enable MPLS FRR on each TE tunnel, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface typeslot/port`
4. `tunnel mode mpls traffic-eng`
5. `tunnel mpls traffic-eng fast-reroute`
6. `end`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface typeslot/port</code>  <b>Example:</b> Router(config)# interface POS1/0	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<code>tunnel mode mpls traffic-eng</code>  <b>Example:</b> Router(config-if)# tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.
Step 5	<code>tunnel mpls traffic-eng fast-reroute</code>  <b>Example:</b> Router(config-if)# tunnel mpls traffic-eng fast-reroute	Enables Fast Reroute on the TE tunnel being protected.
Step 6	<code>end</code>  <b>Example:</b> Router(config-if)# end	Exits to privileged EXEC mode.

## Enabling a Backup Tunnel on an Interface

To enable a backup tunnel on an interface, perform the following steps.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface typeslot/port`
4. `mpls traffic-eng backup-path tunnel interface`
5. `end`

### DETAILED STEPS

Step 1	<code>enable</code>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<code>interface typeslot/port</code>  <b>Example:</b> Router(config)# interface POS1/0	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<code>mpls traffic-eng backup-path tunnel interface</code>  <b>Example:</b> Router(config-if)# mpls traffic-eng backup-path tunnel1	Enables a backup tunnel on a specified interface.
Step 5	<code>end</code>  <b>Example:</b> Router(config-if)# end	Exits to privileged EXEC mode.

## Configuration Examples for the MPLS Traffic Engineering—Fast Reroute MIB

- [Enabling an SNMP Agent on a Host NMS: Example, page 14](#)
- [Enabling Cisco Express Forwarding: Example, page 14](#)
- [Enabling TE Tunnels: Example, page 14](#)
- [Enabling MPLS FRR on Each TE Tunnel: Example, page 15](#)
- [Enabling a Backup Tunnel on an Interface: Example, page 15](#)

### Enabling an SNMP Agent on a Host NMS: Example

The following example shows how to enable an SNMP agent on the host NMS:

```
enable
show running-config
configure terminal
snmp-server community public ro
snmp-server enable traps mpls fast-reroute protected
end
write memory
```

### Enabling Cisco Express Forwarding: Example

The following example shows how to enable Cisco Express Forwarding:

```
enable
configure terminal
ip cef distributed
end
```

### Enabling TE Tunnels: Example

The following example shows how to enable traffic engineering tunnels:

```
enable
configure terminal
```

```
ip cef
mpls traffic-eng tunnels
interface Ethernet1/0
mpls traffic-eng tunnels
end
```

## Enabling MPLS FRR on Each TE Tunnel: Example

The following example shows how to enable MPLS Fast Reroute on each TE tunnel:

```
enable
configure terminal
interface POS1/0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng fast-reroute
end
```

## Enabling a Backup Tunnel on an Interface: Example

The following example shows how to enable a backup tunnel on an interface:

```
enable
configure terminal
interface POS1/0
mpls traffic-eng backup-path tunnel1
end
```

## Additional References

The following sections provide references related to the MPLS Traffic Engineering—Fast Reroute MIB feature.

## Related Documents

Related Topic	Document Title
SNMP agent support for the MPLS Traffic Engineering MIB	<a href="#">MPLS Traffic Engineering MIB</a>
Fast Reroute	<a href="#">MPLS Traffic Engineering (TE): Fast Reroute (FRR) Link and Node Protection</a>

## Standards

Standard	Title
<i>MPLS-FRR-MIB</i>	<i>draft-ietf-mpls-fastreroute-mib-02.txt</i>

## MIBs

MIB	MIBs Link
MPLS Traffic Engineering (TE) MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
No new or modified RFCs are supported by this MIB, and support for existing RFCs has not been modified by this MIB.	—

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This feature uses no new or modified commands.

# Feature Information for MPLS Traffic Engineering—Fast Reroute MIB

Table 5 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(10)ST or Cisco IOS Release 12.0(16)ST or 12.4(20)T or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Table 5** Feature Information for MPLS Traffic Engineering—Fast Reroute MIB

Feature Name	Releases	Feature Information
MPLS Traffic Engineering—Fast Reroute MIB	12.0(10)ST 12.0(16)ST 12.0(22)S 12.0(26)S 12.2(33)SRA 12.2(33)SXH 12.4(20)T	<p>The MPLS Traffic Engineering—Fast Reroute MIB provides SNMP-based network management of the Multiprotocol Label Switching (MPLS) Fast Reroute (FRR) feature in Cisco IOS software.</p> <p>In 12.0(10)ST, the Fast Reroute link protection feature was introduced.</p> <p>In 12.0(16)ST, link protection for Cisco series 7200 and 7500 platforms was added.</p> <p>In 12.0(22)S, Fast Reroute enhancements, including node protection, were added.</p> <p>In 12.0(26)S, support for the IETF MIB <i>draft-ietf-mpls-fastreroute-mib-02.txt</i>, which provides network management for the FRR feature, was added.</p> <p>In 12.2(33)SRA, support for <code>cmplsFrrLogTableCurrEntries</code> and <code>cmplsFrrNotifMaxRate</code> was added. The <code>cmplsFrrLogTable</code> is not supported.</p> <p>In 12.2(33)SXH, support was added.</p> <p>In 12.4(20)T, support was added.</p>



# Glossary

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with large and dynamic traffic patterns.

**index**—A method of uniquely identifying a tunnel.

**instance**—An occurrence. An object can have one or more instances.

**IS-IS**—Intermediate System-to-Intermediate System. IS-IS is an OSI link-state hierarchical routing protocol based on DECnet Phase V routing where intermediate system (IS) routers exchange routing information based on a single metric to determine network topology.

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**LFIB**—Label Forwarding Information Base. The data structure for storing information about incoming and outgoing tags (labels) and associated equivalent packets suitable for labeling.

**LSR**—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as Simple Network Management Protocol (SNMP). The value of a MIB object can be changed or retrieved by using SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**NMS**—network management station. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**notification**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred.

**object**—A variable that has a specific instance associated with it.

**OSPF**—Open Shortest Path First. Link-state, hierarchical Interior Gateway Protocol (IGP) routing algorithm proposed as a successor to Routing Information Protocol (RIP) in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing.

**RSVP**—Resource Reservation Protocol. Protocol for reserving network resources to provide quality of service (QoS) guarantees to application flows.

**scalar object**—Objects that are not instances. A scalar object has one instance.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**SNMP agent**—A managed node or device. The router that has the MIB implementation on it.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2001–2009 Cisco Systems, Inc. All rights reserved.





# MPLS VPN—MIB Support

---

**First Published: March 18, 2002**

**Last Updated: August 26, 2008**

This document describes the Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) management, as implemented in the draft *MPLS/BGP Virtual Private Network Management Information Base Using SMIv2* (*draft-ietf-ppvpn-mpls-vpn-mib-05.txt*). This document also describes the cMplsNumVrfRouteMaxThreshCleared notification, which is implemented as part of the proprietary MIB CISCO-IETF-PPVNP-MPLS-VPN-MIB.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS VPN—MIB Support](#)” section on page 30.

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

## Contents

- [Prerequisites for MPLS VPN—MIB Support, page 2](#)
- [Restrictions for MPLS VPN—MIB Support, page 2](#)
- [Information About MPLS VPN—MIB Support, page 2](#)
- [How to Configure MPLS VPN—MIB Support, page 20](#)
- [Configuration Examples for MPLS VPN—MIB Support, page 26](#)
- [Additional References, page 28](#)
- [Command Reference, page 29](#)
- [Feature Information for MPLS VPN—MIB Support, page 30](#)



---

**Americas Headquarters:**

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

- [Glossary, page 32](#)

## Prerequisites for MPLS VPN—MIB Support

The MPLS VPN MIB agent requires the following:

- SNMP is installed and enabled on the label switching routers.
- MPLS is enabled on the label switching routers.
- Multiprotocol Border Gateway Protocol (BGP) is enabled on the label switching routers.
- Cisco Express Forwarding is enabled on the label switching routers.

## Restrictions for MPLS VPN—MIB Support

The following restrictions apply to the PPVPN-MPLS-VPN MIB:

- Configuration of the MIB using the SNMP SET command is not supported, except for trap-related objects, such as `mplsVpnNotificationEnable` and `mplsVpnVrfSecIllegalLabelRcvThresh`.
- The `mplsVpnVrfBgpNbrPrefixTable` is not supported.

## Information About MPLS VPN—MIB Support

This section contains the following topics:

- [MPLS VPN Overview, page 2](#)
- [MPLS VPN MIB Overview, page 3](#)
- [MPLS VPN MIB and the IETF, page 3](#)
- [Capabilities Supported by PPVPN-MPLS-VPN MIB, page 3](#)
- [Functional Structure of the PPVPN-MPLS-VPN MIB, page 4](#)
- [Supported Objects in PPVPN-MPLS-VPN MIB, page 4](#)
- [Unsupported Objects in PPVPN-MPLS-VPN MIB, page 19](#)

## MPLS VPN Overview

The MPLS VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers. Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF is created for each VPN defined on a router and contains most of the information needed to manage and monitor MPLS VPNs: an IP routing table, a derived Cisco Express Forwarding table, a set of interfaces that use this forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

## MPLS VPN MIB Overview

The Provider-Provisioned VPN (PPVPN)-MPLS-VPN MIB provides access to MPLS VRF information, and interfaces included in the VRF, and other configuration and monitoring information.

The PPVPN-MPLS-VPN MIB provides the following benefits:

- A standards-based SNMP interface for retrieving information about critical MPLS VPN events.
- VRF information to assist in the management and monitoring of MPLS VPNs.
- Information, in conjunction with the Interfaces MIB, about interfaces assigned to VRFs.
- Performance statistics for all VRFs on a router.
- The generation and queueing of notifications that call attention to major changes in the operational status of MPLS VPN enabled interfaces; the forwarding of notification messages to a designated network management system (NMS) for evaluation and action by network administrators.
- Advanced warning when VPN routing tables are approaching or exceed their capacity.
- Warnings about the reception of illegal labels on a VRF-enabled interface. Such receptions may indicate misconfiguration or an attempt to violate security.

This document also describes the CISCO-IETF-PPVPN-MPLS-VPN-MIB, which contains the cMplsNumVrfRouteMaxThreshCleared notification.

## MPLS VPN MIB and the IETF

SNMP agent code operating with the PPVPN-MPLS-VPN MIB enables a standardized, SNMP-based approach to managing MPLS VPNs in Cisco IOS software.

The PPVPN-MPLS-VPN MIB is based on the Internet Engineering Task Force draft MIB specification *draft-ietf-ppvpn-mpls-vpn-mib-05.txt*, which includes objects describing features that support MPLS VPN events. This IETF draft MIB, which undergoes revisions from time to time, is becoming a standard. Accordingly, the Cisco implementation of the PPVPN-MPLS-VPN MIB is expected to track the evolution of the IETF draft MIB, and may change accordingly.

Some slight differences between the IETF draft MIB and the actual implementation of MPLS VPNs within Cisco IOS software require some minor translations between the PPVPN-MPLS-VPN MIB and the internal data structures of Cisco IOS software. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco IOS software. SNMP adds little overhead on the normal functions of the device.

The SNMP objects defined in the PPVPN-MPLS-VPN MIB can be viewed by any standard SNMP utility. The network administrator can retrieve information in the PPVPN-MPLS-VPN MIB using standard SNMP get and getnext operations for SNMP v1, v2, and v3.

All PPVPN-MPLS-VPN MIB objects are based on the IETF draft MIB; thus, no Cisco-specific SNMP application is required to support the functions and operations pertaining to the PPVPN-MPLS-VPN MIB features.

## Capabilities Supported by PPVPN-MPLS-VPN MIB

The PPVPN-MPLS-VPN MIB provides you with the ability to do the following:

- Gather routing and forwarding information for MPLS VPNs on a router.

- Expose information in the VRF routing table.
- Gather information on BGP configuration related to VPNs and VRF interfaces and statistics.
- Emit notification messages that signal changes when critical MPLS VPN events occur.
- Enable, disable, and configure notification messages for MPLS VPN events by using extensions to existing SNMP command-line interface (CLI) commands.
- Specify the IP address of NMS in the operating environment to which notification messages are sent.
- Write notification configurations into nonvolatile memory.

## Functional Structure of the PPVPN-MPLS-VPN MIB

The SNMP agent code supporting the PPVPN-MPLS-VPN MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS software tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure that is common to MIB support code in Cisco IOS software, consists of four layers:

- Platform-independent layer—This layer is generated primarily by the MIB development Cisco IOS software tool set and incorporates platform- and implementation-independent functions. The Cisco IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the MIB development Cisco IOS software tool set.
- Application-specific layer—This layer provides an interface between the application interface layer and the API and data structures layer below and performs tasks needed to retrieve required information from Cisco IOS software, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within Cisco IOS software that are retrieved or called in order to set or retrieve SNMP management information.

## Supported Objects in PPVPN-MPLS-VPN MIB

The PPVPN-MPLS-VPN MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS VPN feature in Cisco IOS software. The PPVPN-MPLS-VPN MIB conforms to Abstract Syntax Notation One (ASN.1), thus reflecting an idealized MPLS VPN database.

Using any standard SNMP network management application, you can retrieve and display information from the PPVPN-MPLS-VPN MIB using GET operations; similarly, you can traverse information in the MIB database for display using GETNEXT operations.

The PPVPN-MPLS-VPN MIB tables and objects are described briefly in the following sections:

- [Scalar Objects, page 6](#)
- [MIB Tables, page 6](#)
- [Notifications, page 16](#)

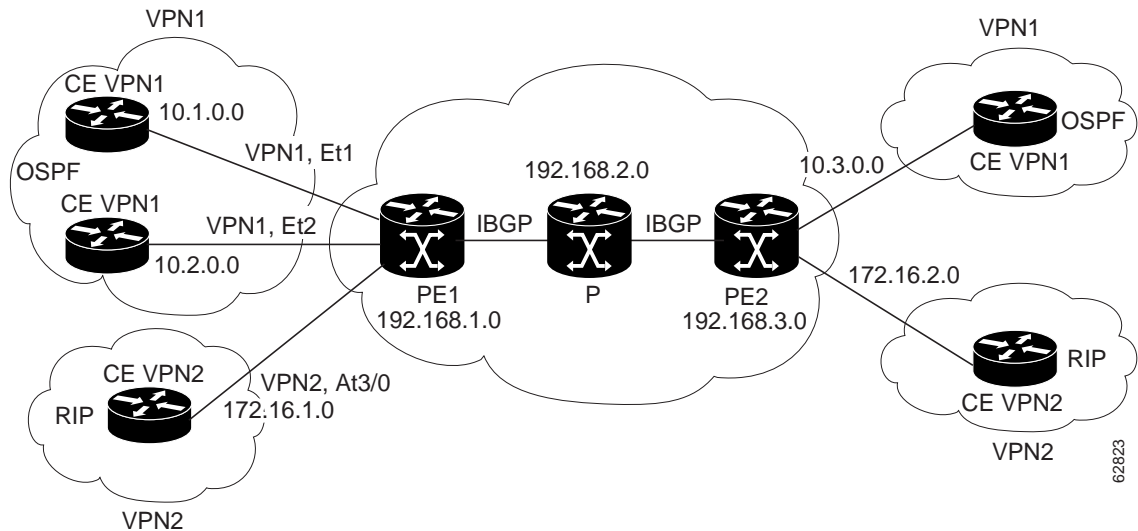
Objects that are not supported are listed in the [“Unsupported Objects in PPVPN-MPLS-VPN MIB” section on page 19](#).

Figure 1 shows a simple MPLS VPN configuration. This configuration includes two customer MPLS VPNs, labeled VPN1 and VPN2, and a simple provider network that consists of two provider edge (PE) routers, labeled PE1 and PE2, and a provider core router labeled P. Figure 1 shows the following sample configuration:

- VRF names—VPN1 and VPN2
- Interfaces associated with VRFs—Et1, Et2, and At3/0
- Routing protocols—Open Shortest Path First. Link-state (OSPF), Routing Information Protocol (RIP), and internal Border Gateway Protocol (IBGP)
- Routes associated with VPN1—10.1.0.0, 10.2.0.0, and 10.3.0.0
- Routes associated with VPN2—172.16.1.0 and 172.16.2.0
- Routes associated with the provider network—192.168.1.0, 192.168.2.0, and 192.168.3.0

This configuration is used in this document to explain MPLS VPN events that are monitored and managed by the PPVPN-MPLS-VPN MIB.

**Figure 1**      **Sample MPLS VPN Configuration**





## Scalar Objects

Table 1 shows the supported PPVPN-MPLS-VPN MIB scalar objects.

**Table 1** *PPVPN-MPLS-VPN MIB Scalar Objects*

MIB Object	Function
<code>mplsVpnConfiguredVrfs</code>	The number of VRFs configured on the router, including VRFs recently deleted.
<code>mplsVpnActiveVrfs</code>	The number of VRFs that are active on the router. An active VRF is assigned to at least one interface that is in the operationally up state.
<code>mplsVpnConnectedInterfaces</code>	The total number of interfaces assigned to any VRF.
<code>mplsVpnNotificationEnable</code>	<p>A value that indicates whether all the PPVPN-MPLS-VPN MIB notifications are enabled:</p> <ul style="list-style-type: none"> <li>Setting this object to true enables all notifications defined in the PPVPN-MPLS-VPN MIB.</li> <li>Setting this object to false disables all notifications defined in the MIB.</li> </ul> <p>This is one of the few objects that is writable.</p>
<code>mplsVpnVrfConfMaxPossibleRoutes</code>	A number that indicates the amount of routes that this router is capable of storing. This value cannot be determined because it is based on the amount of available memory in the system. Therefore, this object is set to zero (0).

## MIB Tables

The PPVPN-MPLS-VPN MIB implementation supports the following tables described in this section:

- [mplsVpnVrfTable](#), page 6
- [mplsVpnInterfaceConfTable](#), page 8
- [mplsVpnVrfRouteTargetTable](#), page 10
- [mplsVpnVrfBgpNbrAddrTable](#), page 12
- [mplsVpnVrfSecTable](#), page 13
- [mplsVpnVrfPerfTable](#), page 13
- [mplsVpnVrfRouteTable](#), page 13

### **mplsVpnVrfTable**

Entries in the VRF configuration table (`mplsVpnVrfTable`) represent the VRFs that are defined on the router. This includes recently deleted VRFs. The information in this table is also displayed with the **show ip vrf** command.

Each VRF is referenced by its VRF name (`mplsVpnVrfName`).

Table 2 lists the MIB objects and their functions for this table.

**Table 2** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfTable*

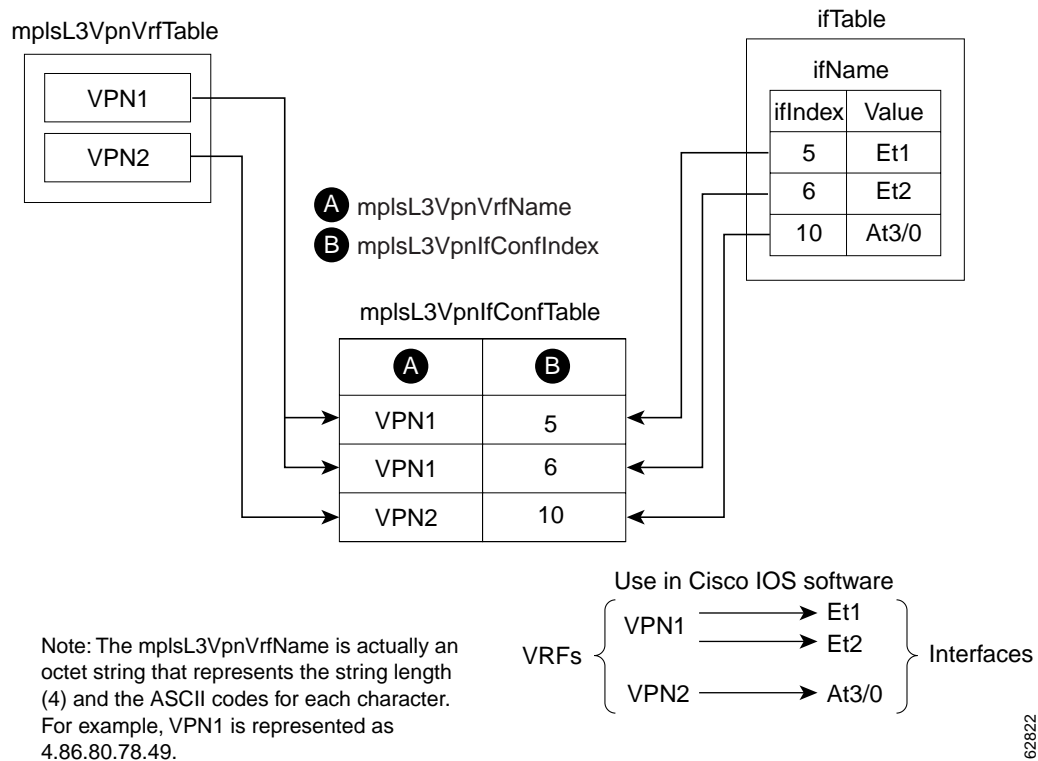
MIB Object	Function
mplsVpnVrfName	The name associated with this VRF. When this object is used as an index to a table, the first octet is the string length, and subsequent octets are the ASCII codes of each character. For example, “vpn1” is represented as 4.118.112.110.49.
mplsVpnVrfDescription	The description of the VRF. This is specified with the following configuration command:  Router(config)# <b>ip vrf</b> <i>vrf-name</i>  Router(config-vrf)# <b>description</b> <i>vrf-description</i>
mplsVpnVrfRouteDistinguisher	The route distinguisher for this VRF. This is specified with the following configuration command:  Router(config)# <b>ip vrf</b> <i>vrf-name</i>  Router(config-vrf)# <b>rd</b> <i>route-distinguisher</i>
mplsVpnVrfCreationTime	The value of the sysUpTime when this VRF entry was created.
mplsVpnVrfOperStatus	The operational status of this VRF. A VRF is up (1) when at least one interface associated with the VRF is up. A VRF is down (2) when: <ul style="list-style-type: none"> <li>No interfaces exist whose ifOperStatus = up (1).</li> <li>No interfaces are associated with this VRF.</li> </ul>
mplsVpnVrfActiveInterfaces	The number of interfaces assigned to this VRF that are operationally up.
mplsVpnVrfAssociatedInterfaces	The number of interfaces assigned to this VRF, independent of the operational status.
mplsVpnVrfConfMidRouteThreshold	The middle route threshold. If the amount of routes in the VRF crosses this threshold, an mplsNumVrfRouteMidThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in configuration mode as a percentage of the maximum with the <b>maximum routes limit</b> { <i>warn-threshold</i>   <b>warn-only</b> } command, as follows:  Router(config)# <b>ip vrf</b> <i>vpn1</i>  Router(config-vrf)# <b>maximum routes</b> 1000 50  The middle or warn threshold is set for VRF vpn1 as 50 percent of the maximum route threshold.  The following command sets a middle threshold of 1000 routes. An mplsNumVrfRouteMidThreshExceeded notification is sent when this threshold is exceeded. However, additional routes are still allowed because a maximum route threshold is not set with this command.  Router(config-vrf)# <b>maximum routes</b> 1000 <b>warn-only</b>

**Table 2** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfTable (continued)*

MIB Object	Function
mplsVpnVrfConfHighRouteThreshold	<p>The maximum route threshold. If the number of routes in the VRF crosses this threshold, an mplsNumVrfRouteMaxThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in configuration mode with the <b>maximum routes limit</b> {<i>warn-threshold</i>   <b>warn-only</b>} command as follows:</p> <pre>Router(config)# ip vrf vpn2</pre> <pre>Router(config-vrf)# maximum routes 1000 75</pre> <p>The maximum route threshold is set for 1000 routes for VRF vpn2 with a middle or warn threshold of 75 percent of this threshold.</p>
mplsVpnVrfConfMaxRoutes	This value is the same as the mplsVpnVrfConfHighRouteThreshold.
mplsVpnVrfConfLastChanged	<p>The value of sysUpTime when the configuration of the VRF changes or interfaces are assigned or unassigned from the VRF.</p> <p><b>Note</b> This object is updated only when values in this table change.</p>
mplsVpnVrfConfRowStatus	Read-only implementation. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted.
mplsVpnVrfConfStorageType	Read-only implementation. This object always reads “volatile (2).”

### mplsVpnInterfaceConfTable

In Cisco IOS software, a VRF is associated with one MPLS VPN. Zero or more interfaces can be associated with a VRF. A VRF uses an interface that is defined in the ifTable of the Interfaces Group of MIB II (IFMIB). The IFMIB defines objects for managing interfaces. The ifTable of this MIB contains information on each interface in the network. The mplsVpnInterfaceConfTable associates a VRF from the mplsVpnVrfTable with a forwarding interface from the ifTable. [Figure 2](#) shows the relationship between VRFs and interfaces defined in the ifTable and the mplsVpnInterfaceConfTable.

**Figure 2** VRFs, the Interfaces MIB, and the *mplsVpnInterfaceConfTable*

Entries in the VPN interface configuration table (*mplsVpnInterfaceConfTable*) represent the interfaces that are assigned to each VRF. The information available in this table is also displayed with the **show ip vrf** command.

The *mplsVpnInterfaceConfTable* shows how interfaces are assigned to VRFs. A label switch router (LSR) creates an entry in this table for every interface capable of supporting MPLS VPNs.

The *mplsVpnInterfaceConfTable* is indexed by the following:

- *mplsVpnVrfName*—The VRF name
- *mplsVpnInterfaceConfIndex*—An identifier that is the same as the *ifIndex* from the Interface MIB of the interface assigned to the VRF

Table 3 lists the MIB objects and their functions for this table.

**Table 3** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnInterfaceConfTable*

MIB Object	Function
mplsVpnInterfaceConfIndex	Provides the interface MIB ifIndex of this interface that is assigned to a VRF.
mplsVpnInterfaceLabelEdgeType	Indicates whether the interface is a provider edge interface (1) or a customer edge interface (2).  This value is always providerEdge (1) because in Cisco IOS software, customerEdge interfaces are not assigned to VRFs and do not appear in this table.
mplsVpnInterfaceVpnClassification	Specifies what type of VPN this interface is providing: carrier supporting carrier (CSC) (1), enterprise (2), or InterProvider (3).  This value is set to enterprise (2) if MPLS is not enabled and to carrier supporting carrier (1) if MPLS is enabled on this interface.
mplsVpnInterfaceVpnRouteDistProtocol	Indicates the route distribution protocols that are being used to redistribute routes with BGP on this interface: BGP (2), OSPF (3), or RIP (4).  In Cisco IOS software, router processes are defined and redistributed on a per-VRF basis, not per-interface. Therefore, all interfaces assigned to the same VRF have the same value for this object.
mplsVpnInterfaceConfStorageType	Read-only implementation. This object always reads “volatile (2).”
mplsVpnInterfaceConfRowStatus	Read-only implementation. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted.

### mplsVpnVrfRouteTargetTable

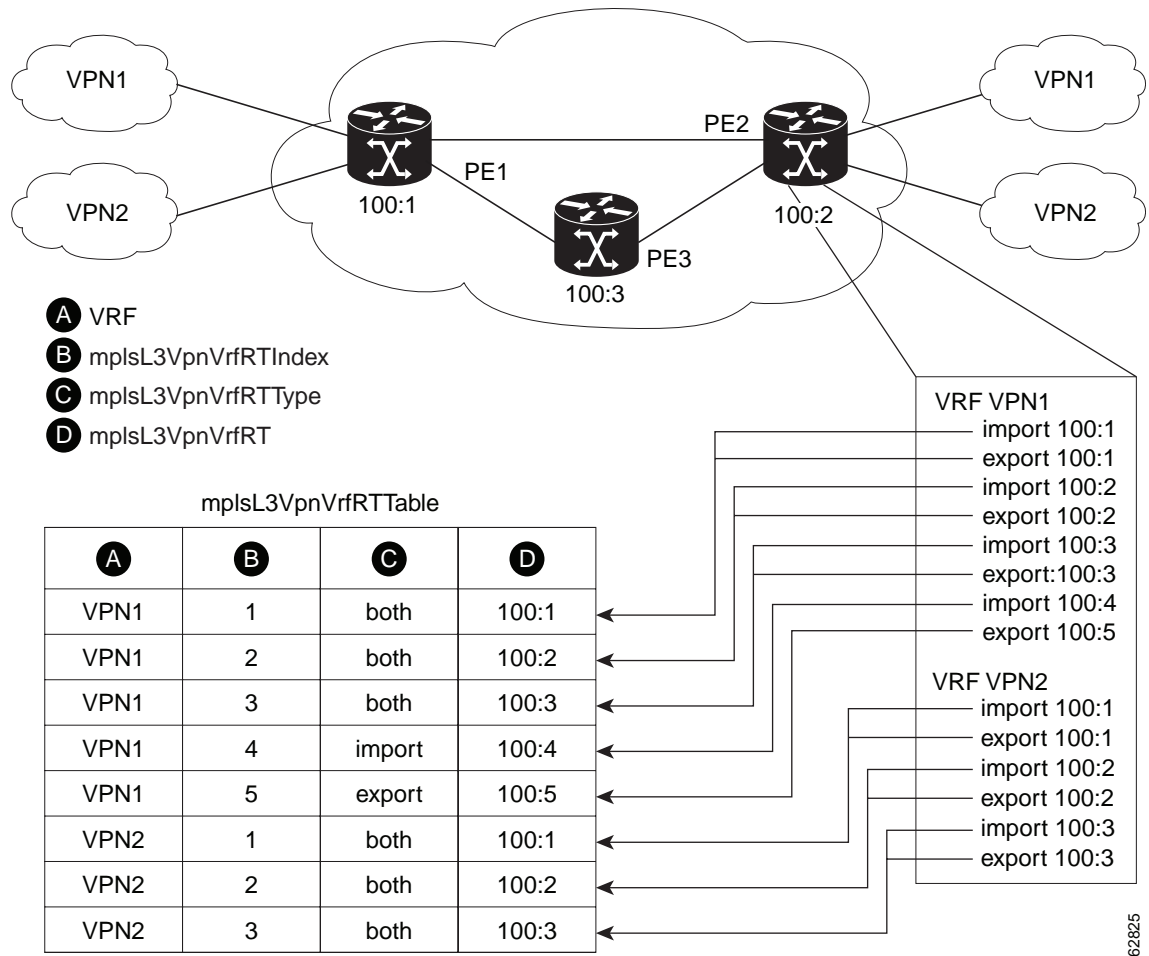
The route target table (mplsVpnVrfRouteTargetTable) describes the route target communities that are defined for a particular VRF. An LSR creates an entry in this table for each target configured for a VRF supporting an MPLS VPN instance.

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

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

Figure 3 shows a sample configuration and its relationship to an mplsVpnVrfRouteTargetTable. A route target table exists on each PE router. Routers with route distinguishers (RDs) 100:1, 100:2, and 100:3 are shown in the sample configuration. Routers with RDs 100:4 and 100:5 are not shown in Figure 3, but are included in the route targets for PE2 and in the mplsVpnVrfRouteTargetTable.

**Figure 3** Sample Configuration and the *mplsVpnVrfRouteTargetTable*



Note: The mplsL3VpnVrfName is actually an octet string that represents the string length (4) and the ASCII codes for each character. For example, VPN1 is represented as 4.86.80.78.49.

The *mplsVpnVrfRouteTargetTable* shows the import and export route targets for each VRF. The table is indexed by the following:

- *mplsVpnVrfName*—The VRF name
- *mplsVpnVrfRouteTargetIndex*—The route target entry identifier
- *mplsVpnVrfRouteTargetType*—A value specifying whether the entry is an import route target, export route target, or is defined as both

Table 4 lists the MIB objects and their functions for this table.

**Table 4** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfRouteTargetTable*

MIB Object	Function
mplsVpnVrfRouteTargetIndex	A value that defines each route target's position in the table.
mplsVpnVrfRouteTargetType	Determines which type of route target the entry represents: import (1), export (2), or both (3).
mplsVpnVrfRouteTarget	Determines the route distinguisher for this target.
mplsVpnVrfRouteTargetDescr	Description of the route target. This object is not supported. Therefore, the object is the same as mplsVpnVrfRouteTarget.
mplsVpnVrfRouteTargetRowStatus	Read-only implementation. This object normally reads "active (1)," but may read "notInService (2)," if a VRF was recently deleted.

### mplsVpnVrfBgpNbrAddrTable

The BGP neighbor address table (mplsVpnVrfBgpNbrAddrTable) represents the MPLS external Border Gateway Protocol (eBGP) neighbors that are defined for a particular VRF. An LSR creates an entry for every BGP neighbor that is defined in the VRF's address-family.

The mplsVpnVrfBgpNbrAddrTable is indexed by the following:

- mplsVpnVrfName—The VRF name
- mplsVpnInterfaceConfIndex—An identifier that is the same as the ifIndex from the Interface MIB of the interface assigned to the VRF
- mplsVpnVrfBgpNbrIndex—The IP address of the neighbor

Table 5 lists the MIB objects and their functions for this table.

**Table 5** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfBgpNbrAddrTable*

MIB Object	Function
mplsVpnVrfBgpNbrIndex	The IPv4 address of the eBGP neighbor.
mplsVpnVrfBgpNbrRole	The role of this eBGP neighbor: customer edge (1) or provider edge (2). If the object mplsVpnInterfaceVpnClassification is CSC, then this value is provider edge (2); otherwise, this value is customer edge (1).
mplsVpnVrfBgpNbrType	Address type of this eBGP neighbor. The MIB supports only IPv4 (1). Therefore, this object returns "ipv4 (1)."
mplsVpnVrfBgpNbrAddr	IP address of the eBGP neighbor.
mplsVpnVrfBgpNbrRowStatus	Read-only implementation. This object normally reads "active (1)," but may read "notInService (2)" if a VRF was recently deleted.
mplsVpnVrfBgpNbrStorageType	Read-only implementation. This object always reads "volatile (2)."

## mplsVpnVrfSecTable

The VRF security table (mplsVpnVrfSecTable) provides information about security for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS VPN.

The mplsVpnVrfSecTable *augments* the mplsVpnVrfTable and has the same indexing.

Table 6 lists the MIB objects and their functions for this table.

**Table 6** PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfSecTable

MIB Object	Function
mplsVpnVrfSecIllegalLabelViolations	<p>The number of illegally received labels on a VRF interface. Only illegal labels are counted by this object, therefore the object only applies to a VRF interface that is MPLS enabled (CSC situation).</p> <p>This counter is incremented whenever a label is received that is above or below the valid label range, not in the global label forwarding table, or is received on the wrong VRF (that is, table IDs for the receiving interface and appropriate VRF label forwarding table do not match).</p>
mplsVpnVrfSecIllegalLabelRcvThresh	<p>Notification threshold for illegal labels received on this VRF. When the number of illegal labels received on this interface crosses this threshold, an mplsNumVrfSecIllegalLabelThreshExceeded notification is sent (if the notification is enabled and configured).</p> <p>This object is one of the few in this MIB agent that supports the SNMP SET operation, which allows you to change this value.</p>

## mplsVpnVrfPerfTable

The VRF performance table (mplsVpnVrfPerfTable) provides statistical performance information for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS VPN.

The mplsVpnVrfPerfTable *augments* the mplsVpnVrfTable and has the same indexing.

Table 7 lists the MIB objects and their functions for this table.

**Table 7** PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfPerfTable

MIB Objects	Functions
mplsVpnVrfPerfRoutesAdded	The number of routes added to this VRF over the course of its lifetime.
mplsVpnVrfPerfRoutesDeleted	The number of routes removed from this VRF.
mplsVpnVrfPerfCurrNumRoutes	The number of routes currently defined within this VRF.

## mplsVpnVrfRouteTable

The VRF routing table (mplsVpnVrfRouteTable) provides the IP routing table information for each VRF. The information available in this table can also be accessed with the **show ip route vrf vrf-name** command. For example, for PE1 in Figure 1:

- With the **show ip route vrf vpn1** command, you would see results like the following:

```
Router# show ip route vrf vpn1
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
```



```

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
    10.0.0.0/32 is subnetted, 3 subnets
B       10.3.0.0 [200/0] via 192.168.2.1, 04:36:33
C       10.1.0.0/16 is directly connected, Ethernet1
C       10.2.0.0/16 [200/0] directly connected Ethernet2, 04:36:33

```

- With the **show ip route vrf vpn2** command, you would see results like the following:

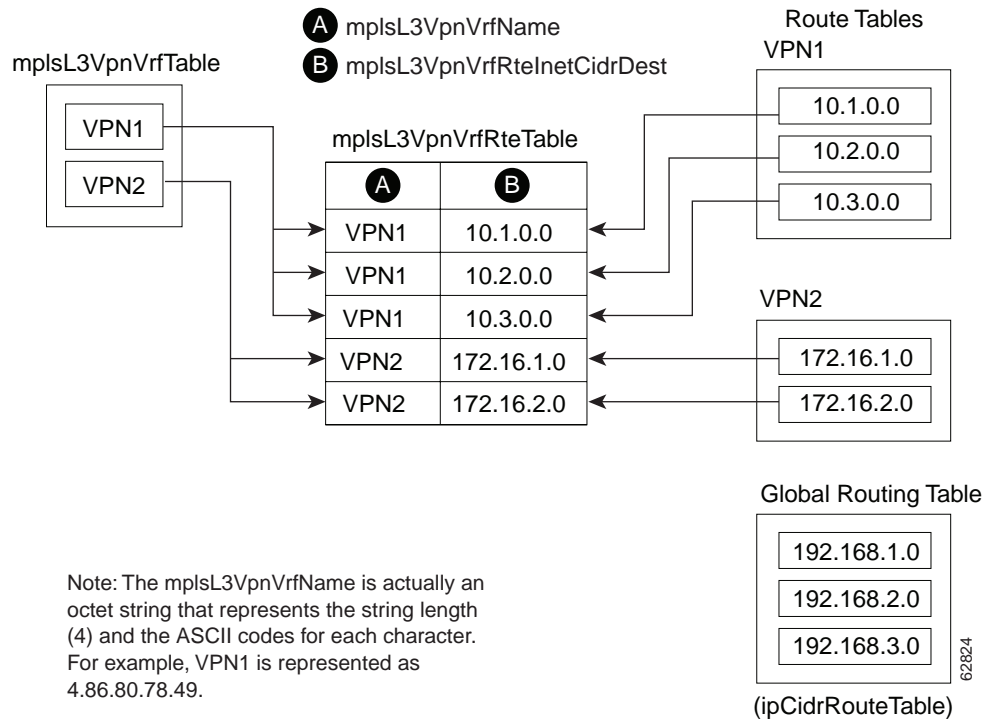
```

Router# show ip route vrf vpn2

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
    172.16.0.0/32 is subnetted, 2 subnets
B       172.16.2.0 [200/0] via 192.168.2.1, 04:36:33
C       172.16.1.0 is directly connected, ATM 3/0

```

Figure 4 shows the relationship of the routing tables, the VRFs, and the `mplsVpnVrfRouteTable`. You can display information about the VPN1 and VPN2 route tables using the **show ip route vrf vrf-name** command. The global route table is the same as `ipCidrRouteTable` in the IP-FORWARD-MIB. You can display information about the global route table with the **show ip route** command.

**Figure 4**      **Route Table, VRFs, and the mplsVpnVrfRouteTable**

An LSR creates an entry in this table for every route that is configured, either dynamically or statically, within the context of a specific VRF capable of supporting MPLS VPN.

The `mplsVpnVrfRouteTable` is indexed by the following:

- `mplsVpnVrfName`—The VRF name, which provides the VRF routing context
- `mplsVpnVrfRouteDest`—The IP destination address
- `mplsVpnVrfRouteMask`—The IP destination mask
- `mplsVpnVrfRouteTos`—The IP header ToS bits
- `mplsVpnVrfRouteNextHop`—The IP address of the next hop for each route entry



#### Note

The ToS bits are not supported and, therefore, are always 0.

Table 8 lists the MIB objects and their functions for the mplsVpnVrfRouteTable. This table represents VRF-specific routes. The global routing table is the ipCidrRouteTable in the IP-FORWARD-MIB.

**Table 8** *PPVPN-MPLS-VPN MIB Objects for the mplsVpnVrfRouteTable*

MIB Object	Function
mplsVpnVrfRouteDest	The destination IP address defined for this route.
mplsVpnVrfRouteDestAddrType	The address type of the IP destination address (mplsVpnVrfRouteDest). This MIB implementation supports only IPv4 (1). Therefore, this object has a value of “ipv4 (1).”
mplsVpnVrfRouteMask	The destination IP address mask defined for this route.
mplsVpnVrfRouteMaskAddrType	The address type of the destination IP address mask. This MIB implementation supports only IPv4 (1). Therefore, this object has a value of “ipv4 (1).”
mplsVpnVrfRouteTos	The ToS bits from the IP header for this route. Cisco IOS software supports only ToS bits of zero. Therefore, the object is always 0.
mplsVpnVrfRouteNextHop	The next hop IP address defined for this route.
mplsVpnVrfRouteNextHopAddrType	The address type of the next hop IP address. This MIB implementation only supports only IPv4 (1). Therefore, this object has a value of “ipv4 (1).”
mplsVpnVrfRouteIfIndex	The interface MIB ifIndex for the interface through which this route is forwarded. The object is 0 if no interface is defined for the route.
mplsVpnVrfRouteType	Defines if this route is a local or remotely defined route.
mplsVpnVrfRouteProto	The routing protocol that was responsible for adding this route to the VRF.
mplsVpnVrfRouteAge	The number of seconds since this route was last updated.
mplsVpnVrfRouteInfo	A pointer to more information from other MIBs. This object is not supported and always returns “nulloid (0.0).”
mplsVpnVrfRouteNextHopAS	The autonomous system number of the next hop for this route. This object is not supported and is always 0.
mplsVpnVrfRouteMetric1	The primary routing metric used for this route.
mplsVpnVrfRouteMetric2 mplsVpnVrfRouteMetric3 mplsVpnVrfRouteMetric4 mplsVpnVrfRouteMetric5	Alternate routing metrics used for this route. These objects are supported only for Cisco Interior Gateway Routing Protocol (IGRP) and Cisco Enhanced Interior Gateway Routing Protocol (EIGRP). These objects display the bandwidth metrics used for the route. Otherwise, these values are set to –1.
mplsVpnVrfRouteRowStatus	Read-only implementation. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted.
mplsVpnVrfRouteStorageType	Read-only implementation. This object always reads “volatile (2).”

## Notifications

This section provides the following information about supported PPVPN-MPLS-VPN MIB notifications:

- [PPVPN-MPLS-VPN MIB Notification Events, page 17](#)
- [Notification Specification, page 18](#)
- [Monitoring the PPVPN-MPLS-VPN MIB Notifications, page 19](#)

## PPVPN-MPLS-VPN MIB Notification Events

The following notifications of the PPVPN-MPLS-VPN MIB are supported:

- **mplsVrfIfUp**—Sent to an NMS when an interface comes up and is assigned a VRF instance.
- **mplsVrfIfDown**—Generated and sent to the NMS when a VRF is removed from an interface or the interface transitions from an operationally “up” state to a “down” state.
- **mplsNumVrfRouteMidThreshExceeded**—Generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the following commands:

```
Router(config)# ip vrf vrf-name
```

```
Router(config-vrf)# maximum routes limit warn-threshold (% of max)
```

The *warn-threshold* argument is a percentage of the maximum routes specified by the *limit* argument. You can also configure a middle threshold with the following command, in which the *limit* argument represents the warning threshold:

```
Router(config-vrf)# maximum routes limit warn-only
```

This notification is sent to the NMS only at the time the threshold is exceeded. (See [Figure 5](#) for a comparison of the warning and maximum thresholds.) Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.

- **MplsNumVrfRouteMaxThreshExceeded**—Generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the *limit* argument of the **maximum routes** commands:

```
Router(config)# ip vrf vrf-name
```

```
Router(config-vrf)# maximum routes limit warn-threshold (% of max)
```

A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another **MplsNumVrfRouteMaxThreshExceeded** notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. (See [Figure 5](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.)



### Note

The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes limit warn-threshold** command.

Prior to implementation of the PPVPN-MPLS-VPN MIB, you were not notified when this threshold (or the warning threshold) was reached.

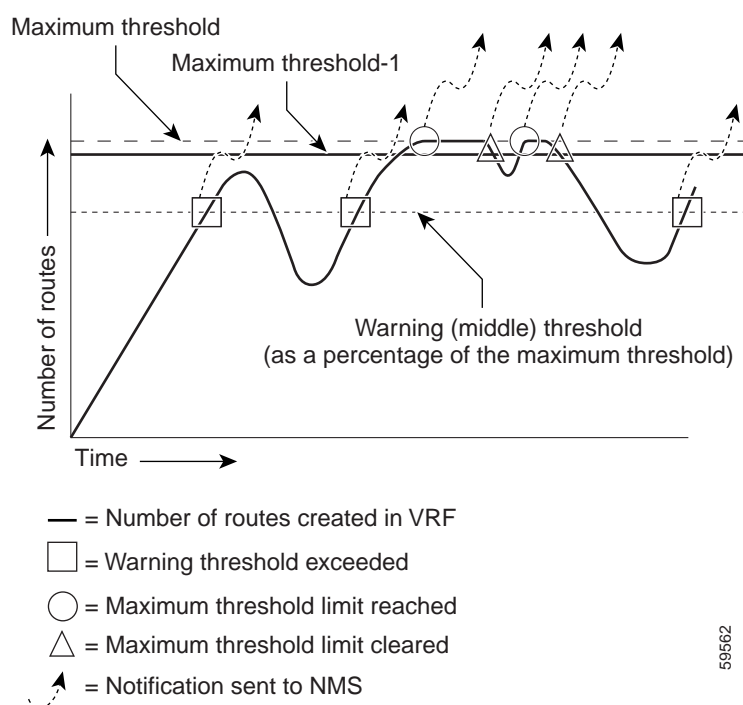
- **mplsNumVrfSecIllegalLabelThreshExceeded**—Generated and sent when the number of illegal labels received on a VRF interface exceeds the threshold *mplsVpnVrfSecIllegalLabelRcvThresh*. This threshold is defined with a value of 0. Therefore, a notification is sent when the first illegal label is received on a VRF. Labels are considered illegal if they are outside of the valid label range, do not have a Label Forwarding Information Base (LFIB) entry, or the table ID of the message does not match the table ID for the label in the LFIB.

## CISCO-IETF-PPVPN-MPLS-VPN MIB Notification Events

The following notification of the CISCO-IETF-PPVPN-MPLS-VPN MIB is supported in Cisco IOS 12.0S releases beginning with Release 12.0(30)S, and in Cisco IOS 12.2S releases beginning with Release 12.2(28)S:

- **cMplsNumVrfRouteMaxThreshCleared**—Generated and sent when the number of routes on a VRF attempts to exceed the maximum number of routes and then drops below the maximum number of routes. **If you attempt to create a route on a VRF that already contains the maximum number of routes, the mplsNumVrfRouteMaxThreshExceeded notification is sent (if enabled). When you remove routes from the VRF so that the number of routes falls below the set limit, the cMplsNumVrfRouteMaxThreshCleared notification is sent.** You can clear all routes from the VRF by using the **clear ip route vrf** command. (See [Figure 5](#) to see when the cMplsNumVrfRouteMaxThreshCleared notification is sent.)

**Figure 5** Comparison of Warning and Maximum Thresholds



For information on the Cisco IOS CLI commands for configuring PPVPN-MPLS-VPN MIB notifications that are to be sent to an NMS, see the [“How to Configure MPLS VPN—MIB Support” section on page 20](#) and the [“Command Reference” section on page 29](#).

## Notification Specification

In an SNMPv1 notification, each VPN notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type.

- The generic type for all VPN notifications is “enterpriseSpecific” because this is not one of the generic notification types defined for SNMP.

- The enterprise-specific type is identified as follows:
  - 1 for *mplsVrflfUp*
  - 2 for *mplsVrflfDown*
  - 3 for *mplsNumVrfRouteMidThreshExceeded*
  - 4 for *mplsNumVrfRouteMaxThreshExceeded*
  - 5 for *mplsNumVrfSecIllegalLabelThreshExceeded*
  - 6 for *cMplsNumVrfRouteMaxThreshCleared*

In SNMPv2, the notification type is identified by an *SnmpTrapOID* varbind (variable binding consisting of an object identifier [OID] type and value) included within the notification message.

Each notification also contains two additional objects from the PPVPN-MPLS-VPN MIB. These objects provide additional information about the event, as follows:

- The VRF interface up/down notifications provide additional variables—*mplsVpnInterfaceConfIndex* and *mplsVpnVrfName*—in the notification. These variables describe the SNMP interface index and the VRF name, respectively.
- The mid and max threshold notifications include the *mplsVpnVrfName* variable (VRF name) and the *mplsVpnVrfPerfCurrNumRoutes* variable that indicates the current number of routes within the VRF.
- The illegal label notification includes the *mplsVpnVrfName* variable (VRF name) and the *mplsVpnVrfSecIllegalLabelViolations* variable that maintains the current count of illegal labels on a VPN.

### Monitoring the PPVPN-MPLS-VPN MIB Notifications

When PPVPN-MPLS-VPN MIB notifications are enabled (see the [snmp-server enable traps mpls vpn](#) command), notification messages relating to specific MPLS VPN events within Cisco IOS software are generated and sent to a specified NMS in the network. Any utility that supports SNMPv1 or SNMPv2 notifications can receive notification messages.

To monitor PPVPN-MPLS-VPN MIB notification messages, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

## Unsupported Objects in PPVPN-MPLS-VPN MIB

The following objects from the *mplsVpnVrfBgpPathAttrTable* are not supported with SNMP management for MPLS VPN features in Cisco IOS software:

- *mplsVpnVrfBgpPathAttrPeer*
- *mplsVpnVrfBgpPathAttrIpAddrPrefixLen*
- *mplsVpnVrfBgpPathAttrIpAddrPrefix*
- *mplsVpnVrfBgpPathAttrOrigin*
- *mplsVpnVrfBgpPathAttrASPathSegment*
- *mplsVpnVrfBgpPathAttrNextHop*
- *mplsVpnVrfBgpPathAttrMultiExitDisc*
- *mplsVpnVrfBgpPathAttrLocalPref*

- `mplsVpnVrfBgpPathAttrAtomicAggregate`
- `mplsVpnVrfBgpPathAttrAggregatorAS`
- `mplsVpnVrfBgpPathAttrAggregatorAddr`
- `mplsVpnVrfBgpPathAttrCalcLocalPref`
- `mplsVpnVrfBgpPathAttrBest`
- `mplsVpnVrfBgpPathAttrUnknown`

## How to Configure MPLS VPN—MIB Support

This section describes configuration tasks for the MPLS VPN—MIB Support feature. Each task in the list is identified as either required or optional.

- [Configuring the SNMP Community, page 20](#) (required)
- [Configuring the Router to Send SNMP Traps, page 22](#) (required)
- [Configuring Threshold Values for MPLS VPN—SNMP Notifications, page 24](#) (required)

The MPLS VPN notifications are enabled or disabled using the extended CLI commands (see the [“Command Reference” section on page 29](#)).

### Configuring the SNMP Community

An SNMP community string defines the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the router.

Perform this task to configure an SNMP community.

#### SUMMARY STEPS

1. **enable**
2. **show running-config** [*options*]
3. **configure terminal**
4. **snmp-server community** *string* [*view view-name*] [*ro* | *rw*] [*acl-number*]
5. **do copy running-config startup-config**
6. **exit**
7. **show-running config** [*interface* | *map-class*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b> [ <i>options</i> ]  <b>Example:</b> Router# show running-config	Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"> <li>If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.</li> </ul>
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <i>acl-number</i> ]  <b>Example:</b> Router(config)# snmp-server community comaccess ro	Sets up the community access string to permit access to the SNMP protocol. <ul style="list-style-type: none"> <li>The <i>string</i> argument acts like a password and permits access to the SNMP protocol.</li> <li>The <b>view</b> <i>view-name</i> keyword argument pair specifies the name of a previously defined view. The view defines the objects available to the community.</li> <li>The <b>ro</b> keyword specifies read-only access. Authorized management stations are only able to retrieve MIB objects.</li> <li>The <b>rw</b> keyword specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.</li> <li>The <i>acl-number</i> argument is an integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.</li> </ul>
Step 5	<b>do copy running-config startup-config</b>  <b>Example:</b> Router(config)# do copy running-config startup-config	Saves the modified configuration to NVRAM as the startup configuration file. <ul style="list-style-type: none"> <li>The <b>do</b> command allows you to perform EXEC level commands in configuration mode.</li> </ul>



	Command or Action	Purpose
Step 6	<code>exit</code>	Returns to privileged EXEC mode.
	<b>Example:</b> <code>Router(config)# exit</code>	
Step 7	<code>show running-config [options]</code>	(Optional) Displays the configuration information currently on the router, the configuration for a specific interface, or map-class information.
	<b>Example:</b> <code>Router# show-running config   include snmp-server</code>	<ul style="list-style-type: none"> <li>Use the <b>show running-config</b> command to check that the <b>snmp-server</b> statements appear in the output.</li> </ul>

## Configuring the Router to Send SNMP Traps

Perform this task to configure the router to sendm SNMP traps to a host.

The **snmp-server host** command specifies which hosts receive traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

For a host to receive a trap, an **snmp-server host** command must be configured for that host, and, generally, the trap must be enabled globally through the **snmp-server enable traps** command.



### Note

Although you can set the *community-string* argument using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
4. **snmp-server enable traps mpls vpn** [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
	<b>Example:</b> <code>Router&gt; enable</code>	
Step 2	<code>configure terminal</code>	Enters global configuration mode.
	<b>Example:</b> <code>Router# configure terminal</code>	

	Command or Action	Purpose
Step 3	<pre>snmp-server host <i>host-addr</i> [<b>traps</b>   <b>informs</b>] [<b>version</b> {1   2c   3 [<b>auth</b>   <b>noauth</b>   <b>priv</b>]}] <i>community-string</i> [<b>udp-port</b> <i>port</i>] [<i>notification-type</i>] [<b>vrf</b> <i>vrf-name</i>]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn</pre>	<p>Specifies the recipient of an SNMP notification operation.</p> <ul style="list-style-type: none"> <li>• The <i>host-addr</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>• The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>• The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>• The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following: <ul style="list-style-type: none"> <li>– <b>1</b> —SNMPv1. This option is not available with informs.</li> <li>– <b>2c</b> —SNMPv2C.</li> <li>– <b>3</b> —SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword (<b>auth</b>, <b>noauth</b>, <b>priv</b>).</li> </ul> </li> <li>• The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> <li>• The <b>udp-port</b> <i>port</i> keyword argument pair names the User Datagram Protocol (UDP) port of the host to use. The default is 162.</li> <li>• The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword argument pair specifies the VRF table that should be used to send SNMP notifications.</li> </ul>

	Command or Action	Purpose
Step 4	<pre>snmp-server enable traps mpls vpn [illegal-label][max-thresh-cleared] [max-threshold][mid-threshold][vrf-down] [vrf-up]</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps mpls vpn vrf-down vrf-up</p>	<p>Enables the router to send MPLS VPN-specific SNMP notifications (traps and informs).</p> <ul style="list-style-type: none"> <li>The <b>illegal-label</b> keyword enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have an LFIB entry, or do not match table IDs for the label.</li> <li>The <b>max-thresh-cleared</b> keyword enables a notification when the number of routes falls below the limit after the maximum route limit was attempted.</li> <li>The <b>max-threshold</b> keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another MplsNumVrfRouteMaxThreshExceeded notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. The max-threshold value is determined by the <b>maximum routes</b> command in VRF configuration mode.</li> <li>The <b>mid-threshold</b> keyword enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.</li> <li>The <b>vrf-down</b> keyword enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.</li> <li>The <b>vrf-up</b> keyword enables a notification for the assignment VRF to an interface that is operational or for the transition of a VRF interface to the operationally up state.</li> </ul>
Step 5	<pre>end</pre> <p><b>Example:</b> Router(config)# end</p>	<p>(Optional) Exits to privileged EXEC mode.</p>

## Configuring Threshold Values for MPLS VPN—SNMP Notifications

Perform this task to configure the following threshold values for MPLS VPN—SNMP notifications:

- The mplsNumVrfRouteMidThreshExceeded notification event is generated and sent when the middle (warning) threshold is crossed. You can configure this threshold in the CLI by using the **maximum routes** command in VRF configuration mode. This notification is sent to the NMS only at the time the threshold is exceeded. Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.
- The mplsNumVrfRouteMaxThreshExceeded notification event is generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the **maximum routes** command in VRF configuration mode. A trap notification is sent to the

NMS when you attempt to exceed the maximum threshold. Another `MplsNumVrfRouteMaxThreshExceeded` notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.

See [Figure 5](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.


**Note**

The **maximum routes** command sets the number of routes for a VRF. You *cannot* exceed the number of routes in the VRF that you set with the **maximum routes limit warn-threshold** command.

Prior to the implementation of the PPVPN-MPLS-VPN MIB, you were not notified when this threshold (or the warning threshold) was reached.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf vrf-name**
4. **maximum routes limit {warn-threshold | warn-only}**
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip vrf vrf-name</b>  <b>Example:</b> Router(config)# ip vrf vpn1	Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument specifies the name assigned to a VRF.</li> </ul>

	Command or Action	Purpose
Step 4	<pre>maximum routes limit {warn-threshold   warn-only}</pre> <p><b>Example:</b></p> <pre>Router(config-vrf)# maximum routes 10000 80</pre>	<p>Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes.</p> <ul style="list-style-type: none"> <li>The <i>limit</i> argument specifies the maximum number of routes allowed in a VRF. The range is from 1 to 4,294,967,295.</li> <li>The <i>warn-threshold</i> argument generates a warning when the number of routes set by the <i>warn-threshold</i> argument is reached and rejects routes that exceed the maximum number set in the <i>limit</i> argument. The warning threshold is a percentage from 1 to 100 of the maximum number of routes specified in the <i>limit</i> argument.</li> <li>The <b>warn-only</b> keyword specifies that a system logging error message is issued when the maximum number of routes allowed for a VRF exceeds the limit threshold. However, additional routes are still allowed.</li> </ul>
Step 5	<pre>end</pre> <p><b>Example:</b></p> <pre>Router(config-vrf)# end</pre>	(Optional) Exits to privileged EXEC mode.

## Configuration Examples for MPLS VPN—MIB Support

This section contains the following configuration examples for the MPLS VPN—MIB Support feature:

- [Configuring the SNMP Community: Examples, page 26](#)
- [Configuring the Router to Send SNMP Traps: Example, page 27](#)
- [Configuring Threshold Values for MPLS VPN—SNMP Notifications: Examples, page 27](#)

### Configuring the SNMP Community: Examples

The following example shows enabling a simple SNMP community group. This configuration permits any SNMP client to access all PPVPN-MPLS-VPN MIB objects with read-only access using the community string comaccess.

```
Router# configure terminal
```

```
Router(config)# snmp-server community comaccess ro
```

Verify that the SNMP master agent is enabled for the MPLS VPN—MIB Support feature:

```
Router# show running-config | include snmp-server
```

```
Building configuration...
```

```
.
```

```
snmp-server community comaccess RO
```



#### Note

If you do not see any “snmp-server” statements, SNMP is not enabled on the router.

## Configuring the Router to Send SNMP Traps: Example

The following example shows you how to enable the router to send MPLS VPN notifications to host 172.20.2.160 using the comaccess community string if a VRF transitions from an up or down state:

```
Router# configure terminal

Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn

Router(config)# snmp-server enable traps mpls vpn vrf-down vrf-up
```

## Configuring Threshold Values for MPLS VPN—SNMP Notifications: Examples

The following example shows how to set a maximum threshold of 10,000 routes and a warning threshold that is 80 percent of the maximum threshold for a VRF named vpn1 on a router:

```
Router(config)# ip vrf vpn1

Router(config-vrf)# maximum routes 10000 80
```

The following example shows how to set a warning threshold of 10,000 routes for a VRF named vpn2 on a router. An error message is generated; however, additional routes are still allowed because a maximum route threshold is not set with this command.

```
Router(config)# ip vrf vpn2

Router(config-vrf)# maximum routes 10000 warn-only
```

# Additional References

The following sections provide additional references related to the MPLS VPN-MIB Support feature.

## Related Documents

Related Topic	Document Title
MPLS VPN configuration tasks	<i><a href="#">Configuring MPLS Layer 3 VPNs</a></i>
Basic MPLS VPN carrier supporting carrier configuration tasks	<i><a href="#">MPLS VPN Carrier Supporting Carrier</a></i>

## Standards

Standard	Title
draft-ietf-ppvpn-mpls-vpn-mib-05	<i><a href="#">MPLS/BGP Virtual Private Network Management Information Base Using SMIv2</a></i>

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>MPLS-VPN-MIB</li> <li>CISCO-IETF-PPVPN-MPLS-VPN-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 2233	<i><a href="#">The Interfaces Group MIB using SMIv2</a></i>
RFC 2547bis	<i><a href="#">BGP/MPLS VPNs</a></i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or the *Cisco IOS Master Command List, All Releases*, at [http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all\\_book.html](http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html).

- **snmp-server enable traps mpls vpn**



## Feature Information for MPLS VPN—MIB Support

[Table 9](#) lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

[Table 9](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 9**      **Feature Information for MPLS VPN—MIB Support**

Feature Name	Releases	Feature Information
MPLS VPN—MIB Support	12.0(21)ST 12.0(22)S 12.2(13)S 12.2(15)T 12.0(24)S1 12.0(25)S 12.0(30)S 12.2(28)SB 12.2(33)SRA 12.2(31)SB2 12.2(33)SXH 12.4(20)T	<p>This feature was introduced into Cisco IOS Release 12.0(21)ST.</p> <p>This feature was integrated into Cisco IOS Release 12.0(22)S.</p> <p>This feature was integrated into Cisco IOS Release 12.2(13)S.</p> <p>The PPVPN-MPLS-VPN MIB notifications were supported in Cisco IOS Release 12.2(13)T. The PPVPN-MPLS-VPN MIB tables were integrated into Cisco IOS Release 12.2(15)T.</p> <p>The feature was implemented for ATM and Frame Relay subinterfaces and integrated into Cisco IOS Release 12.0(24)S1.</p> <p>This feature was integrated into Cisco IOS Release 12.0(25)S.</p> <p>This feature was updated with the MPLS VPN Trap Enhancement feature, which introduced the cMplsNumVrfRouteMaxThreshCleared notification. (See <a href="#">“CISCO-IETF-PPVPN-MPLS-VPN MIB Notification Events, page 18”</a> for more information.) The <b>max-thresh-cleared</b> keyword was added to the <b>snmp-server enable traps mpls vpn</b> command.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SRA.</p> <p>This feature was implemented into Cisco IOS Release 12.2(31)SB2.</p> <p>This feature was implemented into Cisco IOS Release 12.2(33)SXH.</p> <p>This feature was integrated into Cisco IOS Release 12.4(20)T.</p>

# Glossary

**autonomous system**—A collection of networks that share the same routing protocol and that are under the same system administration.

**ASN.1**—Abstract Syntax Notation One. The data types independent of particular computer structures and representation techniques. Described by ISO International Standard 8824.

**BGP**—Border Gateway Protocol. The exterior Border Gateway Protocol used to exchange routing information between routers in separate autonomous systems. BGP uses TCP. Because TCP is a reliable protocol, BGP does not experience problems with dropped or fragmented data packets.

**BGP prefixes**—A route announcement using the BGP. A prefix is composed of a path of autonomous system numbers, indicating which networks the packet must pass through, and the IP block that is being routed. A BGP prefix would look something like: 701 1239 42 206.24.14.0/24. (The /24 part is referred to as a CIDR mask.) The /24 indicates that there are 24 ones in the netmask for this block starting from the left side. A /24 corresponds to the natural mask 255.255.255.0.

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with large and dynamic traffic patterns.

**CE router**—customer edge router. A router on the border between a VPN provider and a VPN customer that belongs to the customer.

**CIDR**—classless interdomain routing. A technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes to reduce the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a two-digit number that represents the subnet mask.

**community**—In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

**community name**—*See* community string.

**community string**—A text string that acts as a password and is used to authenticate messages sent between a managed station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the client. Also called a community name.

**IETF**—Internet Engineering Task Force. A task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC. *See also* ISOC.

**informs**—A type of notification message that is more reliable than a conventional trap notification message, because the informs message notification requires acknowledgment, and a trap notification does not.

**ISOC**—Internet Society. An international nonprofit organization, founded in 1992, that coordinates the evolution and use of the Internet. In addition, ISOC delegates authority to other groups related to the Internet, such as the IAB. ISOC is headquartered in Reston, Virginia (United States).

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

**LFIB**—Label Forwarding Information Base. In the Cisco Label Switching system, the data structure for storing information about incoming and outgoing tags (labels) and associated equivalent packets suitable for labeling.

**LSR**—label switch router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**MPLS interface**—An interface on which MPLS traffic is enabled.

**MPLS VPN**—Multiprotocol Label Switching Virtual Private Network. An IP network infrastructure delivering private network services over a public infrastructure using a Layer 3 backbone. Using MPLS VPNs in a Cisco IOS network provides the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.

For an MPLS VPN solution, an MPLS VPN is a set of provider edge routers that are connected by means of a common “backbone” network to supply private IP interconnectivity between two or more customer sites for a given customer. Each VPN has a set of provisioning templates and policies and can span multiple provider administrative domains (PADs).

**NMS**—network management system. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**notification**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred. *See also* trap.

**PE router**—provider edge router. A router on the border between a VPN provider and a VPN customer that belongs to the provider.

**PPVPN**—Provider-Provisioned VPN. The name of the IETF working group that is developing the PPVPN-MPLS-VPN MIB.

**QoS**—quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

**RSVP**—Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

**RT**—route target. An extended community attribute that identifies a group of routers and, in each router of that group, a subset of forwarding tables maintained by the router that can be populated with a BGP route carrying that extended community attribute. The RT is a 64-bit value by which Cisco IOS discriminates routes for route updates in VRFs.

**SNMP**—Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. *See also* SNMP2.

**SNMP2**—SNMP Version 2. Version 2 of the popular network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. *See also* SNMP.

**traffic engineering**—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps (notifications) are less reliable than inform requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received. *See also* notification.

**VPN**—Virtual Private Network. A group of sites that, as the result of a set of administrative policies, are able to communicate with each other over a shared backbone network. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone. *See also* MPLS VPN.

**VPN ID**—A mechanism that identifies a VPN based on RFC 2685. A VPN ID consists of an Organizational Unique Identifier (OUI), a three-octet hex number assigned by the IEEE Registration Authority, and a VPN index, a four-octet hex number, which identifies the VPN within the company.

**VRF**—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

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

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

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

© 2002,2006 – 2008 Cisco Systems, Inc. All rights reserved.



# MPLS EM—MPLS LDP MIB—RFC 3815

---

**First Published: February 19, 2007**

**Last Updated: April 23, 2009**

The MPLS EM—MPLS LDP MIB - RFC 3815 feature document describes the MIBs that support the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) based on RFC 3815, *Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)*, and describes the differences between RFC 3815 and the MPLS-LDP-MIB based on the Internet Engineering Task Force (IETF) draft Version 8 (draft-ietf-mpls-ldp-08.txt). RFC 3815 and IETF draft Version 8 provide an interface for managing LDP through the use of the Simple Network Management Protocol (SNMP).

In RFC 3815, the content of the MPLS-LDP-MIB is divided into four MIB modules: the MPLS-LDP-STD-MIB, the MPLS-LDP-ATM-STD-MIB, the MPLS-LDP-FRAME-RELAY-STD-MIB, and the MPLS-LDP-GENERIC-STD-MIB.

Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for MPLS EM—MPLS LDP MIB - RFC 3815](#)” section on page 50.

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for MPLS EM—MPLS LDP MIB - RFC 3815, page 2](#)
- [Restrictions for MPLS EM—MPLS LDP MIB - RFC 3815, page 2](#)
- [Information About MPLS EM—MPLS LDP MIB - RFC 3815, page 3](#)
- [How to Configure SNMP for MPLS EM—MPLS LDP MIB - RFC 3815, page 31](#)
- [Configuration Examples for MPLS EM—MPLS LDP MIB - RFC 3815, page 45](#)
- [Additional References, page 47](#)
- [Command Reference, page 49](#)
- [Feature Information for MPLS EM—MPLS LDP MIB - RFC 3815, page 50](#)
- [Glossary, page 52](#)

## Prerequisites for MPLS EM—MPLS LDP MIB - RFC 3815

- SNMP must be installed and enabled on the label switch routers (LSRs) or label edge routers (LERs).
- MPLS must be enabled on the LSRs or LERs.
- LDP must be enabled on the LSRs or LERs.
- Cisco Express Forwarding must be enabled on the LSRs or LERs.

For where to find configuration information for MPLS and LDP, see the [“Related Documents” section on page 47](#).

## Restrictions for MPLS EM—MPLS LDP MIB - RFC 3815

The implementation of the MPLS LDP MIB (RFC 3815) for Cisco IOS Release 12.2(33)SRB is limited to read-only (RO) permission for MIB objects.

The following MPLS-LDP-STD-MIB tables are not implemented for Cisco IOS Release 12.2(33)SRB:

- mplsInSegmentLdpLspTable
- mplsOutSegmentLdpLspTable
- mplsFecTable
- mplsLdpLspFecTable
- mplsLdpSessionPeerAddrTable

The following MPLS-LDP-FRAME-RELAY-STD-MIB tables are not implemented for Cisco IOS Release 12.2(33)SRB:

- mplsLdpEntityFrameRelayTable
- mplsLdpEntityFrameRelayLRTTable
- mplsLdpFrameRelaySessionTable

# Information About MPLS EM—MPLS LDP MIB - RFC 3815

Before you configure SNMP for the MPLS EM—MPLS LDP MIB - RFC 3815 feature you should understand the following concepts:

- [Label Distribution Protocol Overview, page 3](#)
- [MPLS EM—MPLS LDP MIB - RFC 3815 Feature Design and Use, page 4](#)
- [Benefits of Using the MPLS EM—MPLS LDP MIB - RFC 3815 Feature, page 5](#)
- [MPLS LDP MIB \(RFC 3815\) Elements, page 6](#)
- [Events Generating MPLS LDP MIB Notifications, page 10](#)
- [Scalar Objects in the MPLS LDP MIB Modules \(RFC 3815\), page 11](#)
- [MIB Tables in the MPLS-LDP-STD-MIB Module \(RFC 3815\), page 12](#)
- [MIB Tables in the MPLS-LDP-ATM-STD-MIB Module \(RFC 3815\), page 19](#)
- [MIB Table in the MPLS-LDP-GENERIC-STD-MIB Module \(RFC 3815\), page 21](#)
- [VPN Contexts in the MPLS LDP MIB, page 22](#)
- [Differences Between the MPLS-LDP-STD-MIB and the MPLS-LDP-MIB, page 25](#)
- [Differences Between the MPLS-LDP-MIB and the MPLS-LDP-ATM-STD-MIB \(RFC 3815\), page 30](#)
- [Differences Between the MPLS-LDP-MIB and the MPLS-LDP-GENERIC-STD-MIB \(RFC 3815\), page 31](#)

## Label Distribution Protocol Overview

MPLS is a packet forwarding technology that uses a short, fixed-length value called a label in packets to determine the next hop for packet transport through an MPLS network by means of LSRs.

A fundamental MPLS principle is that LSRs in an MPLS network must agree on the definition of the labels being used for packet forwarding operations. Label agreement is achieved in an MPLS network by means of procedures defined in the Label Distribution Protocol (LDP).

LDP operations begin with a discovery (hello) process, during which an LDP entity (a local LSR) finds a cooperating LDP peer in the network and negotiates basic operating procedures between them. The recognition and identification of a peer by means of this discovery process results in a hello adjacency, which represents the context within which label binding information is exchanged between the local LSR and its LDP peer. An LDP function then creates an active LDP session between the two LSRs to effect the exchange of label binding information. The result of this process, when carried to completion with respect to all the LSRs in an MPLS network, is a label switched path (LSP), which constitutes an end-to-end packet transmission pathway between the communicating network devices.

LSRs use LDP to collect, distribute, and label binding information to other LSRs in an MPLS network, thereby enabling the hop-by-hop forwarding of packets in the network along normally routed paths.



## MPLS EM—MPLS LDP MIB - RFC 3815 Feature Design and Use

RFC 3815 defines four MIB modules to support the configuration and monitoring of LDP. The MPLS-LDP-STD-MIB module defines objects that are common to all LDP implementations. To monitor LDP on an LSR or an LER, you need to use this MIB and one of the following Layer 2 MIB modules:

- **MPLS-LDP-GENERIC-STD-MIB**—Use this module and the MPLS-LDP-STD-MIB if the LSR or LER supports LDP that uses the global label space; for example, for Layer 2 Ethernet. This module defines Layer 2 per platform label space objects.
- **MPLS-LDP-ATM-STD-MIB**—Use this module and the MPLS-LDP-STD-MIB if the LSR or LER supports LDP that uses Layer 2 ATM. This module defines Layer 2 ATM objects.
- **MPLS-LDP-FRAME-RELAY-STD-MIB**—Use this module and the MPLS-LDP-STD-MIB if the LSR or LER supports LDP that uses Layer 2 Frame Relay. This module defines Layer 2 Frame Relay objects.

**Note**

The MPLS-LDP-FRAME-RELAY-STD-MIB is not implemented for Cisco IOS Release 12.2(33)SRA.

If the LSR or LER uses LDP that supports Ethernet, ATM, and Frame Relay, then all four MIB modules need to be used by an SNMP agent on the LSR or LER.

The RFC 3815 upgrade to the MPLS-LDP-MIB is implemented to enable standard, SNMP-based network management of the label switching features in Cisco IOS software. Providing this capability requires SNMP agent code to execute on a designated network management station (NMS) in the network. The NMS serves as the medium for user interaction with the network management objects in the MIB.

The SNMP agent is a layered structure that is compatible with Cisco IOS software and presents a network administrative and management interface to the objects in the MPLS LDP MIB and, adds to the rich set of label switching capabilities supported by the Cisco IOS software.

You can use an SNMP agent to access MIB module objects using standard SNMP **get** and **getnext** commands to accomplish a variety of network management tasks. All the objects in the MPLS LDP MIB modules follow the conventions defined in RFC 3815, which defines network management objects in a structured and standardized manner.

Slight differences that exist between the RFC 3815 and the implementation of equivalent functions in the Cisco IOS software require some minor translations between the MPLS LDP MIB objects and the internal data structures of Cisco IOS software. Such translations are accomplished by the SNMP agent, which runs in the background on the NMS workstation as a low priority process.

Cisco IOS Release 12(33)SRB supports the following MPLS LDP MIB-related functions:

- Generating and sending of event notification messages that signal changes in the status of LDP sessions
- Enabling and disabling of event notification messages by means of extensions to existing SNMP command-line interface (CLI) commands
- Specification of the name or the IP address of an NMS workstation in the operating environment to which Cisco IOS event notification messages are to be sent to serve network administrative and management purposes
- Storage of the configuration pertaining to an event notification message in NVRAM of the NMS

The structure of the MPLS LDP MIBs conforms to Abstract Syntax Notation One (ASN.1), thereby forming a highly structured and idealized database of network management objects.

MIB structure is represented by a tree hierarchy. Branches along the tree have short text strings and integers to identify them. Text strings describe object names, and integers allow computer software to encode compact representations of the names.

The MPLS LDP MIB is located on the branch of the Internet MIB hierarchy represented by the object identifier 1.3.6.1.2.1.10.166. This branch can also be represented by its object name `iso.org.dod.internet.mgmt.mib-2.transmission.mplsStdMIB`. The MPLS-LSR-STD-MIB is identified by the object name `mplsLsrStdMIB`, which is denoted by the number 4. Therefore, objects in the MPLS-LDP-STD-MIB can be identified in either of the following ways:

- The object identifier—1.3.6.1.2.1.10.166.4.[MIB-variable]
- The object name—`iso.org.dod.internet.mgmt.mib-2.transmission.mplsStdMIB.mplsLdpStdMIB.[MIB-variable]`

You can use any standard SNMP application to retrieve and display information from the MPLS LDP MIBs by means of standard SNMP GET operations. Similarly, you can traverse and display information in the MIB by means of SNMP GETNEXT operations.

## Benefits of Using the MPLS EM—MPLS LDP MIB - RFC 3815 Feature

The MPLS LDP MIBs (RFC 3815) provide the following benefits:

- Retrieves MIB parameters relating to the operation of LDP entities, such as:
  - Well-known LDP discovery port
  - Maximum transmission unit (MTU)
  - Proposed keepalive timer interval
  - Loop detection
  - Session establishment thresholds
  - Range of Virtual Path Identifier (VPI)-Virtual Channel Identifier (VCI) pairs to be used in forming labels
- Gathers statistics relating to LDP operations, such as:
  - Count of the total established sessions for an LDP entity
  - Count of the total attempted sessions for an LDP entity
- Monitors the time remaining for hello adjacencies
- Monitors the characteristics and status of LDP peers, such as:
  - Internetwork layer address of LDP peers
  - Loop detection of LDP peers
  - Default MTU of the LDP peer
  - Number of seconds the LDP peer proposes as the value of the keepalive interval
- Monitors the characteristics and status of LDP sessions, such as:
  - Displaying the error counters
  - Determining the LDP version being used by the LDP session
  - Determining the keepalive hold time remaining for an LDP session
  - Determining the state of an LDP session (whether the session is active)

- Determining the label ranges for platform-wide and interface-specific sessions
- Determining the ATM parameters

## MPLS LDP MIB (RFC 3815) Elements

The following functional elements of the MPLS LDP MIBs (RFC 3815) are used to perform LDP operations:

- LDP entity—Refers to an instance of LDP for purposes of exchanging label spaces; describes a potential session.
- LDP peer—Refers to a remote LDP entity (that is, a nonlocal LSR).
- LDP session—Refers to an active LDP process between a local LSR and a remote LDP peer.
- Hello adjacency—Refers to the result of an LDP discovery process that affirms the state of two LSRs in an MPLS network as being adjacent to each other (that is, as being LDP peers). When the neighbor is discovered, the neighbor becomes a hello adjacency. An LDP session can be established with the hello adjacency. After the session is established, label bindings can be exchanged between the LSRs.

These MPLS LDP MIB elements are briefly described in the following sections:

- [LDP Entities, page 6](#)
- [LDP Sessions and Peers, page 7](#)
- [LDP Hello Adjacencies, page 9](#)

In effect, the MPLS LDP MIBs provide a network management database that supports real-time access to the various MIB objects within, describing the current state of MPLS LDP operations in the network. This network management information database is accessible by means of standard SNMP commands issued from an NMS in the MPLS LDP operating environment.

The MPLS LDP MIBs support the following network management and administrative activities:

- Retrieving MPLS LDP MIB parameters pertaining to LDP operations
- Monitoring the characteristics and the status of LDP peers
- Monitoring the status of LDP sessions between LDP peers
- Monitoring hello adjacencies in the network
- Gathering statistics regarding LDP sessions

## LDP Entities

An LDP entity is uniquely identified by an LDP identifier that consists of the `mplsLdpEntityLdpId` and the `mplsLdpEntityIndex` (see [Figure 1](#)) objects:

- The `mplsLdpEntityLdpId` consists of the local LSR ID (four octets) and the label space ID (two octets). The label space ID identifies a specific label space available within the LSR.
- The `mplsLdpEntityIndex` consists of the IP address of the peer active hello adjacency, which is the 32-bit representation of the IP address assigned to the peer LSR.

The `mplsLdpEntityProtocolVersion` is a sample object from the `mplsLdpEntityTable`.

Figure 1 shows the following indexing:

- `mplsLdpEntityLdpId` = 10.10.10.10.0.0
- LSR ID = 10.10.10.10
- Label space ID = 0.0

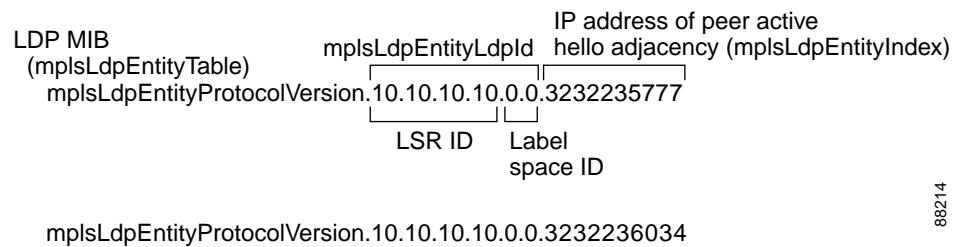


**Note**

The `mplsLdpEntityLdpId` or the LDP ID consists of the LSR ID and the label space ID.

- The IP address of peer active hello adjacency or the `mplsLdpEntityIndex` = 3232235777, which is the 32-bit representation of the IP address assigned to the peer's active hello adjacency.

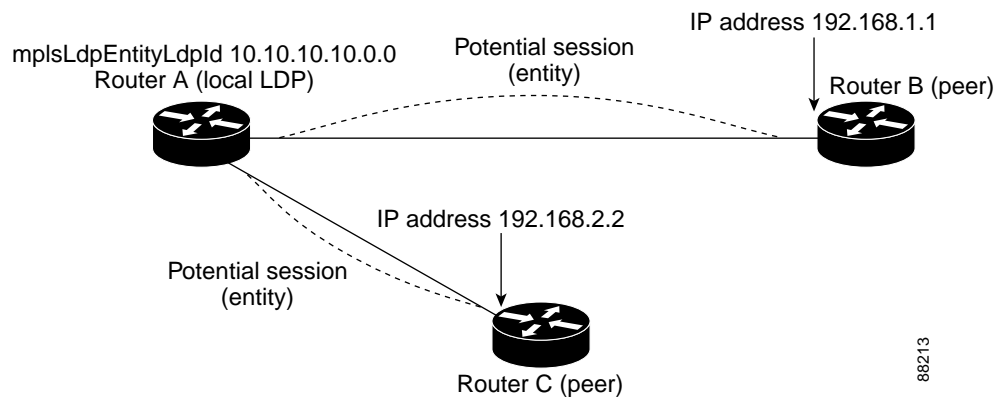
**Figure 1 Sample Indexing for an LDP Entity**



An LDP entity represents a label space that has the potential for a session with an LDP peer. An LDP entity is configured when a hello adjacency receives a hello message from an LDP peer.

In Figure 2, Router A has potential sessions with two remote peers, Routers B and C. The `mplsLdpEntityLdpId` is 10.10.10.10.0.0, and the IP address of the peer active hello adjacency (`mplsLdpEntityIndex`) is 3232235777, which is the 32-bit representation of the IP address 192.168.1.1 for Router B.

**Figure 2 LDP Entity**



## LDP Sessions and Peers

LDP sessions exist between local entities and remote peers for the purpose of distributing label bindings. There is always a one-to-one correspondence between an LDP peer and an LDP session. A single LDP session is an LDP instance that communicates across one or more network links with a single LDP peer.

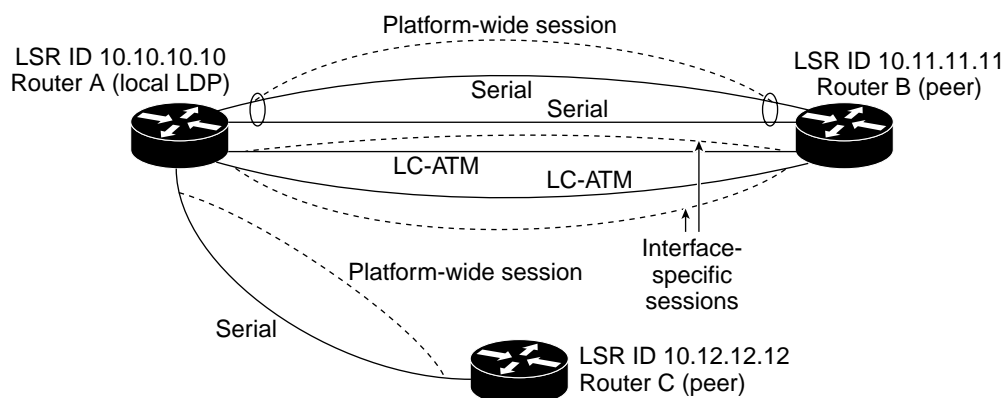
LDP supports the following types of sessions:

- **Interface-specific**—An interface-specific session uses interface resources for label space distributions. For example, each label-controlled ATM (LC-ATM) interface uses its own VPIs and VCIs for label space distributions. Depending on its configuration, an LDP platform can support zero, one, or more interface-specific sessions. Each LC-ATM interface has its own interface-specific label space and a nonzero label space ID.
- **Platform-wide**—An LDP platform supports a single platform-wide session for use by all interfaces that can share the same global label space. For Cisco platforms, all interface types except LC-ATM use the platform-wide session and have a label space ID of zero.

When a session is established between two peers, entries are created in the `mplsLdpPeerTable` and the `mplsLdpSessionTable` because they have the same indexing.

In [Figure 3](#), Router A has two remote peers, Routers B and C. Router A has a single platform-wide session that consists of two serial interfaces with Router B and another platform-wide session with Router C. Router A also has two interface-specific sessions with Router B.

**Figure 3 LDP Sessions**



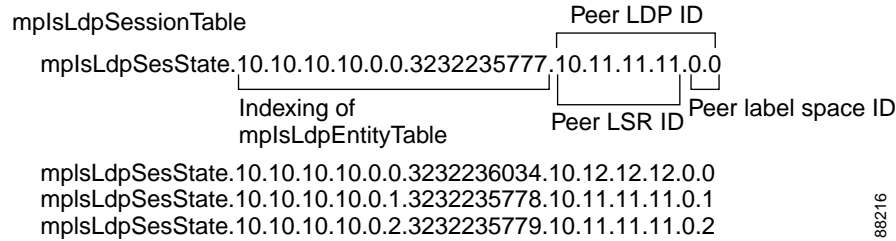
88215

[Figure 4](#) shows entries that correspond to the `mplsLdpPeerTable` and the `mplsLdpSessionTable` in [Figure 3](#).

In [Figure 4](#), `mplsLdpSesState` is a sample object from the `mplsLdpSessionTable` on Router A. Four `mplsLdpSesState` sample objects are shown (top to bottom). The first object represents a platform-wide session associated with two serial interfaces. The next two objects represent interface-specific sessions for the LC-ATM interfaces on Routers A and B. These interface-specific sessions have nonzero peer label space IDs. The last object represents a platform-wide session for the next peer, Router C.

The indexing is based on the entries in the `mplsLdpEntityTable`. It begins with the indexes of the `mplsLdpEntityTable` and adds the following:

- Peer LDP ID = 10.11.11.11.0.0  
The peer LDP ID consists of the peer LSR ID (four octets) and the peer label space ID (two octets).
- Peer LSR ID = 10.11.11.11
- Peer label space ID = 0.0  
The peer label space ID identifies a specific peer label space available within the LSR.

**Figure 4 Sample Indexing for an LDP Session**

88216

## LDP Hello Adjacencies

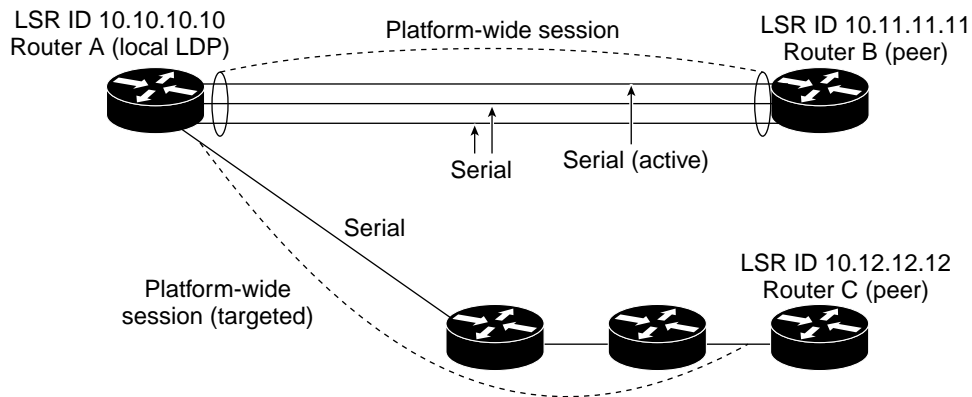
An LDP hello adjacency is an association between a remotely discovered LDP process and a specific network path to reach the remote LDP process. An LDP hello adjacency enables two adjacent peers to exchange label binding information.

An LDP hello adjacency exists for each link on which LDP runs. Multiple LDP hello adjacencies exist whenever there is more than one link in a session between a router and its peer, such as in a platform-wide session.

A hello adjacency is considered active if it is currently engaged in a session, or nonactive if it is not currently engaged in a session.

A targeted hello adjacency is not directly connected to its peer and has an unlimited number of hops between itself and its peer. A linked hello adjacency is directly connected between two routers.

In [Figure 5](#), Router A has two remote peers, Routers B and C. Router A has a platform-wide session with Router B that consists of three serial interfaces, one of which is active and another platform-wide (targeted) session with Router C.

**Figure 5 Hello Adjacency**

88217

[Figure 6](#) shows entries in the mplsLdpHelloAdjacencyTable. There are four mplsLdpHelloAdjHoldTime sample objects (top to bottom). They represent the two platform-wide sessions and the four serial links shown in [Figure 5](#).

The indexing is based on the mplsLdpSessionTable. When the mplsLdpHelloAdjIndex enumerates the different links within a single session, the active link is mplsLdpHelloAdjIndex = 1.

**Figure 6** Sample Indexing for an LDP Hello Adjacency

```

mplsLdpHelloAdjacencyTable
  mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.1
                                     Indexing of mplsLdpSessionTable      mplsLdpHelloAdjIndex
mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.2
mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232235777.10.11.11.11.0.0.3
mplsLdpHelloAdjHoldTimeRem.10.10.10.10.0.0.3232236034.10.12.12.12.0.0.1

```

88218

## Events Generating MPLS LDP MIB Notifications

When you enable MPLS LDP MIB notification functionality by issuing the **snmp-server enable traps mpls rfc ldp** command, notification messages are generated and sent to a designated NMS in the network to signal the occurrence of specific events within Cisco IOS software.

The MPLS LDP MIB objects that announce LDP status transitions and event notifications are the following:

- **mplsLdpSessionUp**—This message is generated when an LDP entity (a local LSR) establishes an LDP session with another LDP entity (an adjacent LDP peer in the network). Enable this notification with the **session-up** keyword.
- **mplsLdpSessionDown**—This message is generated when an LDP session between a local LSR and its adjacent LDP peer is terminated. Enable this notification with the **session-down** keyword.

The up and down notifications indicate the last active interface in the LDP session.

- **mplsLdpPathVectorLimitMismatch**—This message is generated when a local LSR establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits. Enable this notification with the **pv-limit** keyword.

The value of the path vector limit can range from 0 to 255; a value of 0 indicates that loop detection is off; any value other than 0 up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

We recommend that all LDP-enabled routers in the network be configured with the same path vector limit. Accordingly, the **mplsLdpPathVectorLimitMismatch** object exists in the MPLS LDP MIB to provide a warning message to the NMS when two routers engaged in LDP operations have a dissimilar path vector limits.



**Note** This notification is generated only if the distribution method is downstream-on-demand.

- **mplsLdpFailedInitSessionThresholdExceeded**—This message is generated when a local LSR and an adjacent LDP peer attempt to configure an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is eight. This default value is implemented in Cisco IOS software and cannot be changed by either the CLI or an SNMP agent. Enable this notification with the **threshold** keyword.

Eight failed attempts to establish an LDP session between a local LSR and an LDP peer, due to any type of incompatibility between the devices, causes this notification message to be generated.

In general, Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI and VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers try eight times to create an LDP session between themselves before the `mplsLdpFailedInitSessionThresholdExceeded` notification is generated and sent to the NMS as an informational message.

Occasionally, the LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight retry limit is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

**Note**

An `mplsLdpEntityFailedInitSessionThreshold` trap is supported only on an LC-ATM.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers or between Cisco routers and other vendor LSRs in an MPLS network. Among such incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI and VCI ranges (as previously noted) or nonoverlapping Frame Relay data-link connection identifiers (DLCI) ranges between LSRs attempting to configure an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) sizes
- Dissimilar LDP feature support

## Scalar Objects in the MPLS LDP MIB Modules (RFC 3815)

The MPLS LDP MIB modules define several scalar objects. [Table 1](#) describes the scalar objects that are implemented for Cisco IOS Release 12.2(33)SRB.

**Table 1** *MPLS LDP MIB Scalar Objects and Descriptions*

Object	Description
<code>mplsLdpLsrId</code>	The LSR's identifier. This is a globally unique value, such as the 32-bit router ID assigned to the LSR.
<code>mplsLdpLsrLoopDetectionCapable</code>	<p>Loop detection capability of the LSR.</p> <p>Loop detection values are: none(1), other(2), hopCount(3), pathVector(4), and hopCountAndPathVector(5).</p> <p>The other(2) value indicates that the LSR supports loop detection, but does not support the three methods associated with values (3), (4), and (5).</p>
<code>mplsLdpEntityLastChange</code>	The value of <code>sysUpTime</code> at the time of the most recent addition or deletion of an entry to or from the <code>mplsLdpEntityTable</code> or <code>mplsLdpEntityStatsTable</code> , or the most recent change in the value of any object in the <code>mplsLdpEntityTable</code> .



**Table 1** *MPLS LDP MIB Scalar Objects and Descriptions*

Object	Description
mplsLdpEntityIndexNext	Value to use for the mplsLdpEntityIndex when the router creates entries in the mplsLdpEntityTable. The value 0 indicates that no unassigned entries are available.
mplsLdpPeerLastChange	The value of sysUpTime at the time of the most recent addition or deletion to or from the mplsLdpPeerTable or mplsLdpSessionTable.

## MIB Tables in the MPLS-LDP-STD-MIB Module (RFC 3815)

The MPLS-LDP-STD-MIB consists of the following tables. These tables define objects that are common to all LDP implementations.

- mplsLdpEntityTable (see [Table 2](#))—Contains entries for every active LDP hello adjacency. Active and nonactive hello adjacencies appear in the mplsLdpHelloAdjacencyTable, rather than this table. This table is indexed by the local LDP identifier for the interface and the IP address of the peer active hello adjacency. (See [Figure 1](#).)

The advantage of showing the active hello adjacency instead of sessions in this table is that the active hello adjacency can exist even if an LDP session is not active (cannot be established).

Directed adjacencies are also shown in this table. Associated adjacencies disappear when the targeted LDP session fails. Nondirected adjacencies might disappear from the mplsLdpEntityTable on some occasions, because adjacencies are deleted if the underlying interface becomes operationally down, for example.

- mplsLdpEntityStatsTable (see [Table 3](#))—Augments the mplsLdpEntityTable and shares the same indexing for performing SNMP GET and GETNEXT operations. This table shows additional statistics for entities.
- mplsLdpPeerTable (see [Table 4](#))—Contains entries for all peer sessions. This table is indexed by the local LDP identifier of the session, the IP address of the peer active hello adjacency, and the peer's LDP identifier. (See [Figure 4](#).)
- mplsLdpSessionTable (see [Table 5](#))—Augments the mplsLdpPeerTable and shares the same indexing for performing GET and GETNEXT operations. This table shows all sessions.
- mplsLdpSessionStatsTable (see [Table 6](#))—Augments the mplsLdpPeerTable and shares the exact same indexing for performing GET and GETNEXT operations. This table shows additional statistics for sessions.
- mplsLdpHelloAdjacencyTable (see [Table 7](#))—Contains entries for active and nonactive hello adjacencies. This table is indexed by the local LDP identifier of the associated session, the IP address of the peer active hello adjacency, the LDP identifier for the peer, and an arbitrary index that is set to the list position of the adjacency. (See [Figure 6](#).)

## MPLS LDP Entity Table (mplsLdpEntityTable) Objects and Descriptions

Table 2 describes the mplsLdpEntityTable objects.

**Table 2** *mplsLdpEntityTable Objects and Descriptions*

Object	Description
mplsLdpEntityEntry	An LDP entity is a potential session between two peers.
mplsLdpEntityLdpId	The LDP identifier (not accessible) consists of the local LSR ID (four octets) and the label space ID (two octets).
mplsLdpEntityIndex	A secondary index that identifies this row uniquely. It consists of the IP address of the peer active hello adjacency, which is the 32-bit representation of the IP address assigned to the LSR (not accessible).
mplsLdpEntityProtocolVersion	The version number of the LDP protocol to be used in the session initialization message.
mplsLdpEntityAdminStatus	This is the administrative status of this LDP entity, which is always up. If the hello adjacency fails, this entity disappears from the mplsLdpEntityTable.
mplsLdpEntityOperStatus	This is the operational status of this LDP entity. Values are unknown(1), enabled(2), and disabled(3).
mplsLdpEntityTcpPort	This is the TCP discovery port for LDP or Tag Distribution Protocol (TDP). The default value is 646 (LDP).
mplsLdpEntityUdpDscPort	This is the User Datagram Protocol (UDP) discovery port for LDP or TDP. The default value is 646 (LDP).
mplsLdpEntityMaxPduLength	This is the maximum PDU length that is sent in the common session parameters of an initialization message.
mplsLdpEntityKeepAliveHoldTimer	The two-octet value that is the proposed keepalive hold time for this LDP entity.
mplsLdpEntityHelloHoldTimer	The two-octet value that is the proposed hello hold time for this LDP entity.
mplsLdpEntityInitSessionThreshold	The threshold for notification when this entity and its peer are engaged in an endless sequence of initialization messages. <ul style="list-style-type: none"> <li>The default value is 8 and cannot be changed by SNMP or the CLI.</li> </ul>
mplsLdpEntityLabelDistMethod	The specified method of label distribution for any given LDP session. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).
mplsLdpEntityLabelRetentionMode	Can be configured to use either conservative(1) for an LC-ATM or liberal(2) for all other interfaces.

**Table 2** *mplsLdpEntityTable Objects and Descriptions (continued)*

Object	Description
mplsLdpEntityPathVectorLimit	<p>If the value of this object is 0, loop detection for path vectors is disabled. Otherwise, if this object has a value greater than zero, loop detection for path vectors is enabled, and the path vector limit is this value.</p> <p><b>Note</b> The mplsLdpEntityPathVectorLimit object is nonzero only if the mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>
mplsLdpEntityHopCountLimit	<p>If the value of this object is 0, loop detection using hop counters is disabled.</p> <ul style="list-style-type: none"> <li>If the value of this object is greater than 0, loop detection using hop counters is enabled, and this object specifies this entity's maximum allowable value for the hop count.</li> </ul> <p><b>Note</b> The mplsLdpEntityHopCountLimit object is nonzero only if the mplsLdpEntityLabelDistMethod is downstreamOnDemand(1).</p>
mplsLdpEntityTransportAddrKind	<p>If this value is interface(1), the IP address of the interface from the hello message is used as the transport address in the hello message.</p> <p>If this value is loopback(2), the IP address of the loopback interface is used as the address in the hello message.</p>
mplsLdpEntityTargetPeer	If this LDP entity uses a targeted adjacency, this object is set to true(1). The default value is false(2).
mplsLdpEntityTargetPeerAddrType	The type of the internetwork layer address used for the extended discovery. This object indicates how the value of mplsLdpEntityTargPeerAddr is to be interpreted, as either IPv4 or IPv6.
mplsLdpEntityTargetPeerAddr	The value of the internetwork layer address used for the targeted adjacency.
mplsLdpEntityLabelType	<p>Specifies the optional parameters for the LDP initialization message. If the value is generic(1), no optional parameters are sent in the LDP initialization message associated with this entity.</p> <ul style="list-style-type: none"> <li>An LC-ATM uses atmParameters(2) to specify that a row in the mplsLdpEntityAtmParmsTable corresponds to this entry.</li> </ul> <p><b>Note</b> Frame Relay parameters are not supported in Cisco IOS Release 12.2(33)SRB.</p>
mplsLdpEntityDiscontinuityTime	The value of sysUpTime on the most recent occasion when one or more of this entity's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpEntityStatsTable that are associated with this entity. If no such discontinuities have occurred since the last reinitialization of the local management subsystem, this object contains a 0 value.

**Table 2** *mplsLdpEntityTable Objects and Descriptions (continued)*

Object	Description
<code>mplsLdpEntityStorageType</code>	The storage type for this entry is a read-only implementation that is always volatile.
<code>mplsLdpEntityRowStatus</code>	This object is a read-only implementation that is always active.

## MPLS LDP Entity Statistics Table (`mplsLdpEntityStatsTable`) Objects and Descriptions

Table 3 describes the `mplsLdpEntityStatsTable` objects.

**Table 3** *mplsLdpEntityStatsTable Objects and Descriptions*

Object	Description
<code>mplsLdpEntityStatsEntry</code>	These entries augment the <code>mplsLdpEntityTable</code> by providing additional information for each entry.
<code>mplsLdpEntityStatsSessionsAttempts</code>	Not supported in Cisco IOS Release 12.2(33)SRB.
<code>mplsLdpEntityStatsSessionRejectedNoHelloErrors</code>	A count of the session rejected no hello error notification messages sent or received by this LDP entity.
<code>mplsLdpEntityStatsSessionRejectedAdErrors</code>	A count of the session rejected parameters advertisement mode error notification messages sent or received by this LDP entity.
<code>mplsLdpEntityStatsSessionRejectedMaxPduErrors</code>	A count of the session rejected parameters max PDU length error notification messages sent or received by this LDP entity.
<code>mplsLdpEntityStatsSessionRejectedLRErrors</code>	A count of the session rejected parameters label range notification messages sent or received by this LDP entity.
<code>mplsLdpEntityStatsBadLdpIdentifierErrors</code>	A count of the number of bad LDP identifier fatal errors detected by the session associated with this LDP entity.
<code>mplsLdpEntityStatsBadPduLengthErrors</code>	A count of the number of bad PDU length fatal errors detected by the session associated with this LDP entity.
<code>mplsLdpEntityStatsBadMessageLengthErrors</code>	A count of the number of bad message length fatal errors detected by the session associated with this LDP entity.
<code>mplsLdpEntityStatsBadTlvLengthErrors</code>	A count of the number of bad type, length, values (TLVs) length fatal errors detected by the session associated with this LDP entity.
<code>mplsLdpEntityStatsMalformedTlvValueErrors</code>	A count of the number of malformed TLV value fatal errors detected by the session associated with this LDP entity.

**Table 3** *mplsLdpEntityStatsTable Objects and Descriptions (continued)*

Object	Description
mplsLdpEntityStatsKeepAliveTimerExpErrors	A count of the number of session keepalive timer expired errors detected by the session associated with this LDP entity.
mplsLdpEntityStatsShutdownReceivedNotifications	A count of the number of shutdown notifications received related to the session associated with this LDP entity.
mplsLdpEntityStatsShutdownSentNotifications	A count of the number of shutdown notifications sent related to the session associated with this LDP entity.

## MPLS LDP Peer Table (mplsLdpPeerTable) Objects and Descriptions

Table 4 describes the mplsLdpPeerTable objects.

**Table 4** *mplsLdpPeerTable Objects and Descriptions*

Object	Description
mplsLdpPeerEntry	Information about a single peer that is related to a session (not accessible). <b>Note</b> This table is augmented by the mplsLdpSessionTable.
mplsLdpPeerLdpId	The LDP identifier of this LDP peer (not accessible) consists of the peer LSR ID (four octets) and the peer label space ID (two octets).
mplsLdpPeerLabelDistMethod	For any given LDP session, the method of label distribution. Values are downstreamOnDemand(1) and downstreamUnsolicited(2).
mplsLdpPeerPathVectorLimit	If the value of mplsLdpPeerLabelDistMethod is downstreamOnDemand (1), this object represents the path vector limit for this peer. If the value of the mplsLdpPeerLabelDistMethod object is downstreamUnsolicited (2), this value should be 0.
mplsLdpPeerTransportAddrType	Type of Internet address for the mplsLdpPeerTransportAddr object—either the IPv4 transport address or IPv6 transport address used in the opening TCP session or the IPv4 or IPv6 source address for the UDP carrying the hello messages.
mplsLdpPeerTransportAddr	Internet address advertised by the peer in the hello message or the hello source address specified by the mplsLdpPeerTransportAddrType object.

## MPLS LDP Session Table (mplsLdpSessionTable) Objects and Descriptions

Table 5 describes the mplsLdpSessionTable objects.

**Table 5** *mplsLdpSessionTable Objects and Descriptions*

Object	Description
mplsLdpSessionEntry	An entry in this table represents information on a single session between an LDP entity and an LDP peer. The information contained in a row is read-only. This table augments the mplsLdpPeerTable.
mplsLdpSessionStateLastChange	The value of sysUpTime at the time the session entered its state denoted by the mplsLdpSessionState object.
mplsLdpSessionState	<p>The current state of the session. All of the states are based on the LDP or TDP state machine for session negotiation behavior.</p> <p>The states are as follows:</p> <ul style="list-style-type: none"> <li>• nonexistent(1)</li> <li>• initialized(2)</li> <li>• openrec(3)</li> <li>• opensent(4)</li> <li>• operational(5)</li> </ul>
mplsLdpSessionRole	<p>The value of this object indicates whether the LSR or LER takes an active(2) or passive(3) role when a session is established.</p> <p>If the role of the LSR or LER cannot be determined, the value of the object is unknown(1).</p>
mplsLdpSessionProtocolVersion	The version of the LDP protocol that this session is using. This is the version of the LDP protocol that has been negotiated during session initialization.
mplsLdpSessionKeepAliveHoldTimeRem	The keepalive hold time remaining for this session.
mplsLdpSessionKeepAliveTime	The time in seconds between keepalive messages negotiated between a configured value and the peer's proposed keepalive hold timer value. The value is the lower of the two.
mplsLdpSessionMaxPduLen	The value of maximum allowable length for LDP PDUs for this session. This value could have been negotiated during the session initialization.
mplsLdpSessionDiscontinuityTime	<p>The value of sysUpTime on the most recent occasion when one or more of this session's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64 object contained in the mplsLdpSesStatsTable associated with this session.</p> <p>The initial value of this object is the value of sysUpTime when the entry was created in this table.</p>

## MPLS LDP Session Statistics Table (mplsLdpSessionStatsTable) Objects and Descriptions

Table 6 describes the mplsLdpSessionStatsTable objects.

**Table 6** *mplsLdpSessionStatsTable Objects and Descriptions*

Object	Description
mplsLdpSessionStatsEntry	An entry in this table represents statistical information on a single session between an LDP entity and an LDP peer. This table augments the mplsLdpPeerTable.
mplsLdpSessionStatsUnknownMesTypeErrors	This object is the count of the number of unknown message type errors detected during this session.
mplsLdpSessionStatsUnknownTlvErrors	This object is the count of the number of unknown TLV errors detected during this session.

## MPLS LDP Hello Adjacency Table (mplsLdpHelloAdjacencyTable) Objects and Descriptions

Table 7 describes the mplsLdpHelloAdjacencyTable objects.

**Table 7** *mplsLdpHelloAdjacencyTable Objects and Descriptions*

Object	Description
mplsLdpHelloAdjacencyEntry	Each row represents a single LDP hello adjacency. An LDP session can have one or more hello adjacencies (not accessible).
mplsLdpHelloAdjacencyIndex	An identifier for this specific adjacency (not accessible). The active hello adjacency has the mplsLdpHelloAdjIndex object equal to 1.
mplsLdpHelloAdjacencyHoldTimeRem	The time remaining for this hello adjacency. This interval changes when the next hello message, which corresponds to this hello adjacency, is received.
mplsLdpHelloAdjacencyHoldTime	The hello time negotiated between the LSR or LER and its peer.  If this value is 0, the defaults are used, 15 seconds for link hellos and 45 seconds for targeted hellos.  If this value is 65535, the hold time is infinite.
mplsLdpHelloAdjacencyType	This adjacency is the result of a link hello if the value of this object is link(1). Otherwise, this adjacency is a result of a targeted hello and its value is targeted(2).

## MIB Tables in the MPLS-LDP-ATM-STD-MIB Module (RFC 3815)

The MPLS-LDP-ATM-STD-MIB consists of the following tables. These tables define Layer 2 ATM-related objects for use with the MPLS-LDP-STD-MIB.

- `mplsLdpEntityAtmTable` (see [Table 8](#))—Contains entries for every LDP-enabled LC-ATM interface. This table is indexed in the same way as the `mplsLdpEntityTable` although only LC-ATM interfaces are shown.
- `mplsLdpEntityAtmLRTable` (see [Table 9](#))—Contains entries for every LDP-enabled LC-ATM interface. Indexing is the same as it is for the `mplsLdpEntityTable`, except two indexes have been added, `mplsLdpEntityAtmLRMinVpi` and `mplsLdpEntityAtmLRMinVci`. These additional indexes allow more than one label range to be defined. However, in the Cisco IOS Release 12.2(33)SRB implementation, only one label range per LC-ATM interface is allowed.
- `mplsLdpAtmSessionTable` (see [Table 10](#))—Contains entries for LDP-enabled LC-ATM sessions. Indexing is the same as it is for the `mplsLdpPeerTable`, except two indexes have been added, `mplsLdpAtmSessionLRLowerBoundVpi` and `mplsLdpAtmSessionLRLowerBoundVci`. These additional indexes allow more than one label range to be defined. However, in the Cisco IOS Release 12.2(33)SRB implementation, only one label range per LC-ATM interface is allowed.

### MPLS LDP Entity ATM Table (`mplsLdpEntityAtmTable`) Objects and Descriptions

[Table 8](#) describes the `mplsLdpEntityAtmTable` objects.

**Table 8** *`mplsLdpEntityAtmTable` Objects and Descriptions*

Object	Description
<code>mplsLdpEntityAtmEntry</code>	Represents the ATM parameters and ATM information for this LDP entity.
<code>mplsLdpEntityAtmIfIndxOrZero</code>	This value represents the SNMP IF-MIB index for the interface-specific LC-ATM entity.
<code>mplsLdpEntityAtmMergeCap</code>	Denotes the merge capability of this entity.
<code>mplsLdpEntityAtmLRComponents</code>	Number of label range components in the initialization message. This also represents the number of entries in the <code>mplsLdpEntityConfAtmLRTable</code> that correspond to this entry. <b>Note</b> Cisco IOS software supports only one component.
<code>mplsLdpEntityAtmVcDirectionality</code>	If the value of this object is <code>bidirectional(0)</code> , a given VCI within a given VPI is used as a label for both directions independently of one another. If the value of this object is <code>unidirectional(1)</code> , a given VCI within a VPI designates one direction.
<code>mplsLdpEntityAtmLsrConnectivity</code>	The peer LSR can be connected indirectly by means of an ATM VPI, so that the VPI values can be different on the endpoints. For that reason, the label must be encoded entirely within the VCI field. Values are <code>direct(1)</code> and <code>indirect(2)</code> . The default is <code>direct(1)</code> .
<code>mplsLdpEntityAtmDefaultControlVpi</code>	The default VPI value for the non-MPLS connection.



**Table 8** *mplsLdpEntityAtmTable Objects and Descriptions (continued)*

Object	Description
mplsLdpEntityAtmDefaultControlVci	The default VCI value for the non-MPLS connection.
mplsLdpEntityAtmUnlabTrafVpi	VPI value of the virtual channel connector (VCC) supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.
mplsLdpEntityAtmUnlabTrafVci	VCI value of the VCC supporting unlabeled traffic. This non-MPLS connection is used to carry unlabeled (IP) packets.
mplsLdpEntityAtmStorageType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityAtmRowStatus	This object is a read-only implementation that is always active.

## MPLS LDP Entity ATM Label Range Table (mplsLdpEntityAtmLRTable) Objects and Descriptions

Table 9 describes the mplsLdpEntityAtmLRTable objects.

**Table 9** *mplsLdpEntityAtmLRTable Objects and Descriptions*

Object	Description
mplsLdpEntityAtmLREntry	A row in the LDP Entity Configurable ATM Label Range Table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary (VPI/VCI pair) and a lower boundary (VPI/VCI pair). This is the same data used in the initialization message. This label range should overlap the label range of the peer.
mplsLdpEntityAtmLRMinVpi	The minimum VPI number configured for this range (not accessible).
mplsLdpEntityAtmLRMinVci	The minimum VCI number configured for this range (not accessible).
mplsLdpEntityAtmLRMaxVpi	The maximum VPI number configured for this range (not accessible).
mplsLdpEntityAtmLRMaxVci	The maximum VCI number configured for this range (not accessible).
mplsLdpEntityAtmLRStorageType	The storage type for this entry is a read-only implementation that is always volatile.
mplsLdpEntityAtmLRRowStatus	This object is a read-only implementation that is always active.

## MPLS LDP ATM Session Table (mplsLdpAtmSessionTable) Objects and Descriptions

Table 10 describes the mplsLdpAtmSessionTable objects.

**Table 10** *mplsLdpAtmSessionTable Objects and Descriptions*

Objects	Description
mplsLdpAtmSessionEntry	An entry in this table represents information on a single label range intersection between an LDP entity and an LDP peer (not accessible).
mplsLdpAtmSessionLRLowerBoundVpi	The minimum VPI number configured for this range (not accessible).
mplsLdpAtmSessionLRLowerBoundVci	The minimum VCI number configured for this range (not accessible).
mplsLdpAtmSessionLRUpperBoundVpi	The maximum VPI number configured for this range (read-only).
mplsLdpAtmSessionLRUpperBoundVci	The maximum VCI number configured for this range (read-only).

## MIB Table in the MPLS-LDP-GENERIC-STD-MIB Module (RFC 3815)

The MPLS-LDP-GENERIC-STD-MIB contains the following table. This table defines Layer 2 per-platform objects for use with the MPLS-LDP-STD-MIB.

- mplsLdpEntityGenericLRTable (Table 11)—Contains entries for every LDP-enabled interface that is in the global label space. (For Cisco, this applies to all interfaces except LC-ATM. LC-ATM entities are shown in the mplsLdpEntityAtmLRTable instead.) Indexing is the same as it is for the mplsLdpEntityTable, except two indexes have been added, mplsLdpEntityGenericLRMin and mplsLdpEntityGenericLRMax. These additional indexes allow more than one label range to be defined. However, in the Cisco IOS Release 12.2(33)SRB implementation, only one global label range is allowed.

## MPLS LDP Entity Generic Label Range Table (mplsLdpEntityGenericLRTable) Objects and Descriptions

Table 11 describes the mplsLdpEntityGenericLRTable objects.

**Table 11** *mplsLdpEntityGenericLRTable Objects and Descriptions*

Object	Description
mplsLdpEntityGenericLREntry	A row in the LDP Entity Configurable Generic Label Range table. One entry in this table contains information on a single range of labels; the range is defined by an upper boundary and a lower boundary. <ul style="list-style-type: none"> <li>• The current implementation supports one label range per entity.</li> </ul>
mplsLdpEntityGenericLRMin	The minimum label configured for this range (not accessible).

**Table 11** *mplsLdpEntityGenericLRTTable Objects and Descriptions (continued)*

Object	Description
<code>mplsLdpEntityGenericLRMax</code>	The maximum label configured for this range (not accessible).
<code>mplsLdpEntityGenericLabelSpace</code>	This value indicates whether the label space type is perPlatform (1) or perInterface (2).
<code>mplsLdpEntityGenericIfIndxOrZero</code>	This value represents the SNMP IF-MIB index for the platform-wide entity. If the active hello adjacency is targeted, the value is 0.
<code>mplsLdpEntityGenericLRStorageType</code>	The storage type for this entry is a read-only implementation that is always volatile.
<code>mplsLdpEntityGenericLRRowStatus</code>	This object is a read-only implementation that is always active.

## VPN Contexts in the MPLS LDP MIB

Within an MPLS Border Gateway Protocol (BGP) 4 Virtual Private Network (VPN) environment, separate LDP processes can be created for each VPN. These processes and their associated data are called LDP contexts. Each context is independent from all others and contains data specific only to that context.

The VPN Aware LDP MIB feature enables the LDP MIB to get VPN context information. The feature adds support for different contexts for different MPLS VPNs. Users of the MIB can display MPLS LDP processes for a given MPLS VPN. The VPN Aware LDP MIB feature does not change the syntax of the MPLS LDP MIB. It changes the number and types of entries within the tables.

The MPLS LDP MIB can show information about only one context at a time. With Cisco IOS Release 12.2(33)SRB, you can specify a context—either a global context or an MPLS VPN context—using an SNMP security name.

The following sections describe topics related to the VPN Aware LDP MIB feature:

- [SNMP Contexts, page 22](#)
- [VPN Aware LDP MIB Sessions, page 23](#)
- [VPN Aware LDP MIB Notifications, page 24](#)

## SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

VPN-aware SNMP requires that SNMP manager and agent entities operating in a VPN environment agree on mapping between the SNMP security name and the VPN name. This mapping is created by you using different contexts for the SNMP data of different VPNs, which is accomplished through the configuration of the SNMP View-based Access Control Model MIB (SNMP-VACM-MIB). The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space within the context of only that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values within a VPN context:

- The first security phase is authentication of the username. During this phase, the user is authorized for SNMP access.
- The second phase is access control. During this phase, the user is authorized for SNMP access to the group objects in the requested SNMP context.
- In the third phase, the user can access a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VPN routing and forwarding (VRF) instances and SNMP community strings. When a VRF instance is associated with an SNMP community string, SNMP processes requests coming in for a particular community string only if they are received from the configured VRF. If the community string contained in the incoming packet does not have a VRF associated with it, it is processed only if it came in through a non-VRF interface.

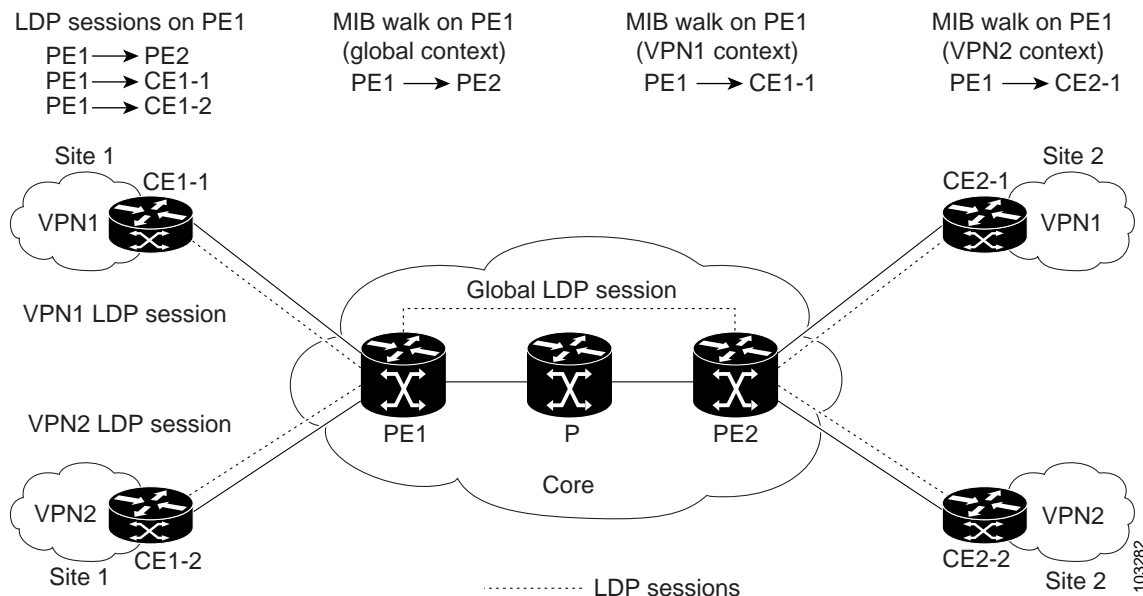
You can also enable or disable authentication traps for SNMP packets dropped due to VRF mismatches. By default, if SNMP authentication traps are enabled, VRF authentication traps are also enabled.

## VPN Aware LDP MIB Sessions

The VPN Aware LDP MIB feature supports an SNMP query to the MPLS LDP MIB for both global and VPN contexts. This feature allows you to enter LDP queries on any VRF and on the core (global context). A query can differentiate between LDP sessions from different VPNs. LDP session information for a VPN stays in the context of that VPN. Therefore, the information from one VPN is not available to a user of a different VPN. The VPN Aware LDP MIB also allows you to display LDP processes operating in a Carrier Supporting Carrier (CSC) network.

In an MPLS VPN, a service provider edge router (PE) might contain VRFs for several VPNs and a global routing table. To set up separate LDP processes for different VPNs on the same device, you need to configure each VPN with a unique `securityName`, `contextName`, and View-based Access Control Model (VACM) view. The VPN `securityName` must be configured for the MPLS LDP MIB.

[Figure 7](#) shows LDP sessions for a sample MPLS VPN with the VPN Aware LDP MIB feature.

**Figure 7 MPLS LDP Sessions with the VPN Aware LDP MIB Feature**

With the VPN Aware LDP MIB feature, you can do MIB queries or MIB walks for an MPLS VPN LDP session or a global LDP session.

**Note**

To verify LDP session information for a specific VPN, use the **show mpls ldp neighbor vrf vpn-name detail** command.

## VPN Aware LDP MIB Notifications

The VPN Aware LDP MIB feature supports LDP notifications for multiple LDP contexts for VPNs. LDP notifications can be generated for the core (global context) and for different VPNs. You can cause notifications be sent to different NMS hosts for different LDP contexts. LDP notifications associated with a specific VRF are sent to the NMS designated for that VRF. LDP global notifications are sent to the NMS configured to receive global traps.

To enable LDP context notifications for the VPN Aware LDP MIB feature, use either the SNMP `mplsLdpSessionsUpDownEnable` object (in the global LDP context only) or the following extended global configuration commands.

To enable LDP notifications for the global context, use the following commands on a provider edge (PE) router:

```
Router(config)# snmp-server host host-address traps community mpls-ldp
```

```
Router(config)# snmp-server enable traps mpls rfc ldp
```

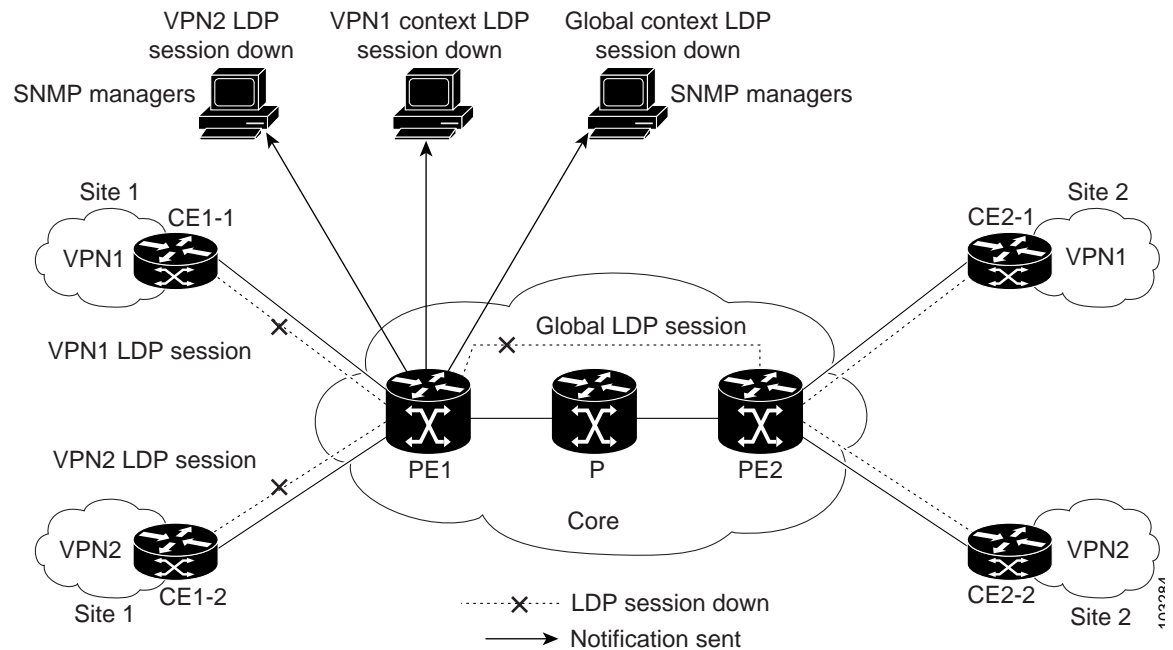
To enable LDP notifications for a VPN context, use the following commands:

```
Router(config)# snmp-server host host-address vrf vrf-name version {v1|v2c|v3}
community community-string udp-port upd-port mpls-ldp
```

```
Router(config)# snmp-server enable traps mpls rfc ldp
```

Figure 8 shows LDP notifications with the VPN Aware LDP MIB feature.

**Figure 8** LDP Notifications with the VPN Aware LDP MIB Feature



## Differences Between the MPLS-LDP-STD-MIB and the MPLS-LDP-MIB

The MPLS-LDP-STD-MIB based on RFC 3815 provides the same basic functionality as the MPLS-LDP-MIB based on the IETF Version 8 draft (draft-ietf-mpls-ldp-08.txt). The module identity was changed from `mplsLdpMIB` to `mplsLdpStdMIB`. Both MIBs provide an interface for managing LDP through the use of SNMP.

After the implementation of the MPLS-LDP-STD-MIB (RFC 3815) in Cisco IOS Release 12.2(33)SRB the MPLS-LDP-MIB will exist for a period of time before support is completely removed. This gives you the chance to migrate to the MPLS-LDP-STD-MIB. Both MIBs can coexist in the same image because the MPLS-LDP-STD-MIB and the MPLS-LDP-MIB have different root object identifiers (OIDs).

The following sections contain information about the major differences between the MPLS-LDP-STD-MIB and the MPLS-LDP-MIB:

- [MPLS-LDP-MIB and MPLS-LDP-STD-MIB Scalar Object Differences, page 25](#)
- [MPLS-LDP-MIB and MPLS-LDP-STD-MIB Table Object Differences, page 26](#)
- [MPLS-LDP-MIB and MPLS-LDP-STD-MIB Notification Changes, page 29](#)

## MPLS-LDP-MIB and MPLS-LDP-STD-MIB Scalar Object Differences

Table 12 shows the difference between the scalar objects in the MPLS-LDP-MIB and the MPLS-LDP-STD-MIB.

**Table 12** *Scalar Objects: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences*

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
—	mplsLdpPeerLastChange	New Object—Indicates the value of the sysUpTime at the time of the most recent addition or deletion to or from the mplsLdpPeerTable or the mplsLdpSessionTable.
mplsLdpSesUpDownTrapEnable	—	Object deleted.
—	mplsFecLastChange <b>Note</b> Not supported in Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB.	New object—Contains the sysUpTime at the time of the most recent change to the mplsLdpFecTable.
—	mplsLdpLspFecLastChange <b>Note</b> Not supported in Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB.	New object—Stores the last change time for the mplsLdpLspFecTable.
—	mplsLdpEntityLastChange	New object—Indicates the last change time for the mplsLdpEntityTable or mplsLdpEntityStatsTable.

## MPLS-LDP-MIB and MPLS-LDP-STD-MIB Table Object Differences

The following tables show the major differences between the MPLS-LDP-MIB and the MPLS-LDP-STD-MIB objects for each table.

### MPLS LDP Entity Table (mplsLdpEntityTable) Differences

[Table 13](#) shows the major differences between MPLS-LDP-MIB and MPLS-LDP-STD-MIB objects for the MPLS LDP entity table.

**Table 13** *MPLS LDP Entity Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences*

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpEntityIndexNext	mplsLdpEntityIndexNext	Syntax changed—Unsigned32 to IndexIntegerNextFree.
mplsLdpEntityIndex	mplsLdpEntityIndex	Syntax changed—Unsigned32 to IndexInteger.
mplsLdpEntityProtocolVersion	mplsLdpEntityProtocolVersion	Syntax changed—Unsigned32 to Integer32.
mplsLdpEntityAdminStatus	mplsLdpEntityAdminStatus	Description changed—Modified to suggest that an NMS clean up any related entry in the mplsLdpPeerTable in case this object is changed from enable to disable.

**Table 13** *MPLS LDP Entity Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences (continued)*

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpEntityOperStatus	mplsLdpEntityOperStatus	Description changed—Modified to include the value of unknown(1) for a transient condition before the LSR changes the value to enabled(2) or disabled(3).
mplsLdpEntityTcpDscPort	mplsLdpEntityTcpPort	Object name changed.
mplsLdpEntityMaxPduLength	mplsLdpEntityMaxPduLength	Syntax changed—Lower-limit value for this object increased from 0 to 256.  Description changed—Indicates that the receiving LSR should calculate the maximum PDU length for the session by using the smaller of its and its peer's proposal for the Max PDU length.
mplsLdpEntityInitSessionThreshold	mplsLdpEntityInitSessionThreshold	Syntax changed—Maximum value changed from MAXINT to 100.
mplsLdpEntityLabelDistMethod	mplsLdpEntityLabelDistMethod	Syntax changed—INTEGER to MplsLabelDistributionMethod TC.
mplsLdpEntityLabelRetentionMode	mplsLdpEntityLabelRetentionMode	Syntax changed—INTEGER to MplsRetentionMode TC.
mplsLdpEntityPVLmisTrapEnable	—	Notification control object removed.
mplsLdpEntityPVL	mplsLdpEntityPathVectorLimit	Object name changed.
mplsLdpEntityHopCountLimit	mplsLdpEntityHopCountLimit	DEFVAL clause added for a default value = 0.
—	mplsLdpEntityTransportAddrKind	New object—Indicates the address to be used for hello messages (interface and loopback).
mplsLdpEntityTargPeerAddrType	mplsLdpEntityTargPeerAddrType	Syntax changed—To InetAddressType.
mplsLdpEntityTargPeerAddr	mplsLdpEntityTargPeerAddr	Syntax changed—To InetAddress.
mplsLdpEntityOptionalParameters	mplsLdpEntityLabelType	Object name changed.
mplsLdpEntityStorType	mplsLdpEntityStorageType	Object name changed.
mplsLdpEntityRowStatus	mplsLdpEntityRowStatus	Description change—Added recommendation to set the mplsLdpEntityAdminStatus to down, change the objects in this entry, and then set the Admin status to enable.

**MPLS LDP Entity Statistics Table (mplsLdpEntityStatsTable) Differences****Note**

A general paragraph regarding discontinuities is added to all the counter objects in MPLS LDP entity statistics table: “Discontinuities in the value of this counter can occur at re-initialization of the management system, and at other times as indicated by the value of mplsLdpEntityDiscontinuityTime.”



Table 14 shows the difference between MPLS-LDP-MIB and MPLS-LDP-STD-MIB objects for the MPLS LDP entity statistics table.

**Table 14 MPLS LDP Entity Statistics Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences**

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpAttemptedSessions	mplsLdpEntityStatsSessionAttempts	Object name changed.
mplsLdpSesRejectedNoHelloErrors	mplsLdpEntityStatsSessionRejectedNoHelloErrors	Object name changed.
mplsLdpSesRejectedAdErrors	mplsLdpEntityStatsSessionRejectedAdErrors	Object name changed.
mplsLdpSesRejectedMaxPduErrors	mplsLdpEntityStatsSessionRejectedMaxPduErrors	Object name changed.
mplsLdpSesRejectedLRErrors	mplsLdpEntityStatsSessionRejectedLRErrors	Object name changed.
mplsLdpBadLdpIdentifierErrors	mplsLdpEntityStatsBadLdpIdentifierErrors	Object name changed.
mplsLdpBadPduLengthErrors	mplsLdpEntityStatsBadPduLengthErrors	Object name changed.
mplsLdpBadMessageLengthErrors	mplsLdpEntityStatsBadMessageLengthErrors	Object name changed.
mplsLdpBadTlvLengthErrors	mplsLdpEntityStatsBadTlvLengthErrors	Object name changed.
mplsLdpMalformedTlvValueErrors	mplsLdpEntityStatsMalformedTlvValueErrors	Object name changed.
mplsLdpKeepAliveTimerExpErrors	mplsLdpEntityStatsKeepAliveTimerExpErrors	Object name changed.
mplsLdpShutdownNotifReceived	mplsLdpEntityStatsShutdownReceivedNotifications	Object name changed.
mplsLdpShutdownNotifSent	mplsLdpEntityStatsShutdownSentNotifications	Object name changed.

### MPLS LDP Peer Table (mplsLdpPeerTable) Differences

Table 15 shows the difference between MPLS-LDP-MIB and MPLS-LDP-STD-MIB objects for the MPLS LDP peer table.

**Table 15 MPLS LDP Peer Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences**

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpPeerLabelDistMethod	mplsLdpPeerLabelDistMethod	Syntax change—From INTEGER to MplsLabelDistributionMethod
mplsLdpPeerLoopDectionForPV	—	Object deleted.
mplsLdpPeerPVL	mplsLdpPeerPathVectorLimit	Object name changed.
—	mplsLdpPeerTransportAddrType	New object—Internet address type (IPv4 or IPv6) advertised by the peer in the hello message or hello source message.
—	mplsLdpPeerTransportAddr	New object—Internet address (IPv4 or IPv6) advertised by the peer in the hello message or hello source message.

## MPLS LDP Session Table (mplsLdpSessionTable) Differences

Table 16 shows the difference between MPLS-LDP-MIB and MPLS-LDP-STD-MIB objects for the MPLS LDP session table.

**Table 16** *MPLS LDP Session Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences*

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpSesState	mplsLdpSessionState	Object name changed.
mplsLdpSesProtocolVersion	mplsLdpSessionProtocolVersion	Object name changed.
—	mplsLdpSessionStateLastChange	New Object—Indicates the last change time for this table.
—	mplsLdpSessionRole	New object—Indicates the LSR state: active, passive, or unknown.
mplsLdpSesKeepAliveHoldTimeRem	mplsLdpSessionKeepAliveHoldTimeRem	Object name changed.
—	mplsLdpSessionKeepAliveTime	New object—Indicates the actual keepalive time negotiated between peers.
mplsLdpSesMaxPduLen	mplsLdpSessionMaxPduLen	Object name changed.
mplsLdpSesDiscontinuityTime	mplsLdpSessionDiscontinuityTime	Object name changed.

## MPLS LDP Hello Adjacency Table (mplsLdpHelloAdjacencyTable) Differences

Table 17 shows the difference between MPLS-LDP-MIB and MPLS-LDP-STD-MIB objects for the MPLS LDP hello adjacency table.

**Table 17** *MPLS LDP Hello Adjacency Table: MPLS-LDP-MIB and MPLS-LDP-STD-MIB Object Differences*

MPLS-LDP-MIB Object	MPLS-LDP-STD-MIB Object	Difference
mplsLdpHelloAdjIndex	mplsLdpHelloAdjacencyIndex	Object name changed.
mplsLdpHelloAdjHoldTimeRem	mplsLdpHelloAdjacencyHoldTimeRem	Object name changed.
—	mplsLdpHelloAdjacencyHoldTime	New object—Indicates the actual negotiated adjacency hold time.
mplsLdpHelloAdjType	mplsLdpHelloAdjacencyType	Object name changed.

## MPLS-LDP-MIB and MPLS-LDP-STD-MIB Notification Changes

All notifications from the MPLS-LDP-MIB are retained in the MPLS-LDP-STD-MIB. The following changes are implemented for the notifications in MPLS-LDP-STD-MIB:

- The mplsLdpPVLMismatch notification is renamed to mplsLdpPathVectorLimitMismatch.
- The mplsLdpEntityPVLMisTrapEnable, notification control object, was removed for the MPLS-LDP-STD-MIB.
- The Cisco IOS command for enabling notifications for the MPLS-LDP-MIB is different from the command for enabling notifications for the MPLS-LSR-STD-MIB.

For the MPLS-LDP-MIB, the command is **snmp-server enable traps mpls ldp**. For the MPLS-LSR-STD-MIB, the command is **snmp-server enable traps mpls rfc ldp**.

## Differences Between the MPLS-LDP-MIB and the MPLS-LDP-ATM-STD-MIB (RFC 3815)

Layer 2 ATM-related objects are removed from the MPLS-LDP-MIB and placed in a new MIB module in RFC 3815. The new MIB module is the MPLS-LDP-ATM-STD-MIB. This action provides modularity and reduces the size of the MPLS LDP MIB.

Table 18 lists the differences between ATM-related objects in the MPLS-LDP-MIB and objects in the MPLS-LDP-ATM-STD-MIB.

**Table 18** *Differences Between MPLS-LDP-MIB and MPLS-LDP-ATM-STD-MIB Objects*

MPLS-LDP-MIB Object	MPLS-LDP-ATM-STD-MIB Object	Difference
mplsLdpEntityAtmParmsTable	mplsLdpEntityAtmTable	Object name changed.
mplsLdpEntityAtmMergeCap	mplsLdpEntityAtmMergeCap	Syntax changed—Added enumerations vpMerge and vpAndVcMerge.
mplsLdpEntityDefaultControlVpi	mplsLdpEntityAtmDefaultControlVpi	Object name changed.
mplsLdpEntityDefaultControlVci	mplsLdpEntityAtmDefaultControlVci	Object name changed.
mplsLdpEntityUnlabTrafVpi	mplsLdpEntityAtmUnlabTrafVpi	Object name changed.
mplsLdpEntityUnlabTrafVci	mplsLdpEntityAtmUnlabTrafVci	Object name changed.
mplsLdpEntityAtmStorType	mplsLdpEntityAtmStorageType	Object name changed.
mplsLdpEntityAtmRowStatus	mplsLdpEntityAtmRowStatus	Description changed—Clarified different row status operations. Added a recommendation that the mplsLdpEntityAdminStatus object be set to down before the LSR changes the objects in this table.
mplsLdpEntityConfAtmLRTable	mplsLdpEntityAtmLRTable	Object name changed.
mplsLdpEntityConfAtmLREntry	mplsLdpEntityAtmLREntry	Object name changed.
mplsLdpEntityConfAtmLRMinVpi	mplsLdpEntityAtmLRMinVpi	Object name changed. Description changed—0 added as a valid value.
mplsLdpEntityConfAtmLRMinVci	mplsLdpEntityAtmLRMinVci	Object name changed.
mplsLdpEntityConfAtmLRMaxVpi	mplsLdpEntityAtmLRMaxVpi	Object name changed.
mplsLdpEntityConfAtmLRMaxVci	mplsLdpEntityAtmLRMaxVci	Object name changed.
mplsLdpEntityConfAtmLRStorType	mplsLdpEntityAtmLRStorageType	Object name changed.
mplsLdpEntityConfAtmLRRowStatus	mplsLdpEntityAtmLRRowStatus	Object name changed.
mplsLdpAtmSesTable	mplsLdpAtmSessionTable	Object name changed.
mplsLdpSesAtmLRLowerBoundVpi	mplsLdpSessionAtmLRLowerBoundVpi	Object name changed.
mplsLdpSesAtmLRLowerBoundVci	mplsLdpSessionAtmLRLowerBoundVci	Object name changed.
mplsLdpSesAtmLRUpperBoundVpi	mplsLdpSessionAtmLRUpperBoundVpi	Object name changed.
mplsLdpSesAtmLRUpperBoundVci	mplsLdpSessionAtmLRUpperBoundVci	Object name changed.

## Differences Between the MPLS-LDP-MIB and the MPLS-LDP-GENERIC-STD-MIB (RFC 3815)

Layer 2 objects for per-platform label spaces are removed from the MPLS-LDP-MIB and placed in a new MIB module in RFC 3815. The new MIB module is the MPLS-LDP-GENERIC-STD-MIB. This action provides modularity and reduces the size of the MPLS LDP MIB.

[Table 19](#) shows the difference between generic label space objects in the MPLS-LDP-MIB and objects in the MPLS-GENERIC-STD-MIB.

**Table 19** *MPLS LDP LSP DEC Table: MPLS-LDP-MIB and MPLS-LDP-GENERIC-STD-MIB Object Differences*

MPLS-LDP-MIB Object	MPLS-LDP-GENERIC-STD-MIB Object	Difference
mplsLdpEntityConfGenLRTable	mplsLdpEntityGenericLRTable	Object name changed.
mplsLdpEntityConfGenLRMin	mplsLdpEntityGenericLRMin	Object name changed.
mplsLdpEntityConfGenLRMax	mplsLdpEntityGenericLRMax	Object name changed.
mplsLdpEntityConfGenIfIndexOrZero	mplsLdpEntityGenericIfIndexOrZero	Object name changed.
mplsLdpEntityConfGenLRStorType	mplsLdpEntityGenericLRStorageType	Object name changed.
mplsLdpEntityConfGenLRRowStatus	mplsLdpEntityGenericRowStatus	Object name changed.
—	mplsLdpEntityGenericLabelSpace	New object—A value of perPlatform(1) indicates the label space type is per platform; a value of perInterface(2) indicates the label space type is per interface.

## How to Configure SNMP for MPLS EM—MPLS LDP MIB - RFC 3815

To configure SNMP for the MPLS EM—MPLS LDP MIB - RFC 3815 feature, perform the following tasks:

- [Configuring Access to an SNMP Agent on a Host NMS Workstation, page 31](#) (required)
- [Configuring the Router to Send SNMP Notifications to a Host for Monitoring LDP, page 33](#) (required)
- [Configuring a VPN-Aware LDP MIB, page 35](#) (optional)

### Configuring Access to an SNMP Agent on a Host NMS Workstation

To configure access to the SNMP agent on a host NMS workstation, perform the following task.

Through the use of an SNMP agent, the MPLS LDP MIBs described in RFC 3815 provide an interface for monitoring and managing LDP.

To use SNMP to manage LDP, you need to configure access to an SNMP agent on a NMS workstation. By default, the SNMP agent for the MPLS LDP MIB is disabled. Step 2 shows you how to determine if an SNMP agent is already configured, and if you need to modify the SNMP information to monitor and manage LDP.

## SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*acl-number*]
5. **do copy running-config startup-config**
6. **exit**
7. **show-running config**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"> <li>• If no SNMP information is displayed, continue with the next step. If any SNMP information is displayed, you can modify the information or change it as needed.</li> </ul>
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <i>acl-number</i> ]  <b>Example:</b> Router(config)# snmp-server community comaccess ro	Configures the community access string to permit access to the SNMP protocol. <ul style="list-style-type: none"> <li>• The <i>string</i> argument acts like a password and permits access to the SNMP protocol.</li> <li>• The <b>view</b> <i>view-name</i> keyword argument pair specifies the name of a previously defined view. The view defines the objects available to the community.</li> <li>• The <b>ro</b> keyword specifies read-only access. Authorized management stations are able to only retrieve MIB objects.</li> <li>• The <b>rw</b> keyword specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.</li> <li>• The <i>acl-number</i> argument is an integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.</li> </ul>

	Command or Action	Purpose
Step 5	<code>do copy running-config startup-config</code>  <b>Example:</b> <pre>Router(config)# do copy running-config startup-config</pre>	(Optional) Saves the modified configuration to nonvolatile memory (NVRAM) as the startup configuration file. <ul style="list-style-type: none"> <li>• Use this command if you made changes to the MIB information.</li> <li>• The <b>do</b> command allows you to perform EXEC-level commands in configuration modes.</li> </ul>
Step 6	<code>exit</code>  <b>Example:</b> <pre>Router(config)# exit</pre>	Returns to privileged EXEC mode.
Step 7	<code>show running-config</code>  <b>Example:</b> <pre>Router# show running-config   include snmp-server</pre>	(Optional) Displays the configuration information currently on the router. <ul style="list-style-type: none"> <li>• Use the <b>show running-config</b> command to check that the <b>snmp-server</b> command statements appear in the output.</li> </ul>

## Examples

Use the **show running-config** command to display the running configuration on the host NMS workstation and examine the output for SNMP information. For example:

```
Router# show running-config | include snmp-server

snmp-server community public RO
snmp-server community private RW
```

The presence of any **snmp-server** command statement in the output that takes the form shown in this example verifies that access to the SNMP agent is configured on the host NMS workstation.

## Configuring the Router to Send SNMP Notifications to a Host for Monitoring LDP

To configure the router to send SNMP notifications to a host to monitor LDP, perform the following task. The ability to display SNMP notifications helps in managing LDP sessions. You can determine if an LDP session between peers is up or down, if the path vector limits are the same for both LDP peers, and if the path vector limit threshold between the peers has been exceeded.

The **snmp-server host** command specifies which hosts receive notifications or traps. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified traps.

For a host to receive a trap, an **snmp-server host** command must be configured for that host, and, generally, the trap must be enabled globally through the **snmp-server enable traps** command.

## Prerequisites

Although you can set the *community-string* argument using the **snmp-server host** command by itself, we recommend that you define this string using the **snmp-server community** command prior to using the **snmp-server host** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
4. **snmp-server enable traps mpls ldp** [**pv-limit**] [**session-down**] [**session-up**] [**threshold**]
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server host</b> <i>host-address</i> [ <b>traps</b>   <b>informs</b> ] [ <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}] <i>community-string</i> [ <b>udp-port</b> <i>port</i> ] [ <i>notification-type</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-ldp	Specifies the recipient of an SNMP notification operation. <ul style="list-style-type: none"> <li>• The <i>host-address</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>• The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>• The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>• The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following: <ul style="list-style-type: none"> <li>– <b>1</b>—SNMPv1. This option is not available with informs.</li> <li>– <b>2c</b>—SNMPv2C.</li> <li>– <b>3</b>—SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword: <b>auth</b>, <b>noauth</b>, <b>priv</b>.</li> </ul> </li> <li>• The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> </ul>

Command or Action	Purpose
<p><b>Step 4</b></p> <pre>snmp-server enable traps mpls ldp [pv-limit] [session-down] [session-up] [threshold]</pre> <p><b>Example:</b>  Router(config)# snmp-server enable traps mpls  rfc ldp session-down</p>	<ul style="list-style-type: none"> <li>• The <b>udp-port</b> <i>port</i> keyword argument pair names the UDP port of the host to use. The default is 162.</li> <li>• The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword argument pair specifies the VRF table that should be used to send SNMP notifications.</li> </ul> <p>Enables the router to send MPLS LDP-specific SNMP notifications (traps and informs) defined in RFC 3815.</p> <ul style="list-style-type: none"> <li>• The <b>pv-limit</b> keyword controls (enables or disables) path-vector (PV) limit notifications (mplsLdpPathVectorLimitMismatch). This notification is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path-vector limits.</li> <li>• The <b>session-down</b> keyword controls (enables or disables) LDP session down notifications (mplsLdpSessionDown). This message is generated when an LDP session between the router and its adjacent LDP peer is terminated.</li> <li>• The <b>session-up</b> keyword controls (enables or disables) LDP session up notifications (mplsLdpSessionUp). This notification is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).</li> <li>• The <b>threshold</b> keyword controls (enables or disables) PV limit notifications (mplsLdpFailedInitSessionThresholdExceeded). This notification is generated after eight failed attempts to establish an LDP session between the router and an LDP peer. The failure can be the result of any type of incompatibility between the devices.</li> </ul>
<p><b>Step 5</b></p> <pre>end</pre> <p><b>Example:</b>  Router(config)# end</p>	<p>(Optional) Exits to privileged EXEC mode.</p>

## Configuring a VPN-Aware LDP MIB

To configure a VPN-aware LDP MIB, perform the following tasks:

- [Configuring SNMP Support for a VPN, page 36](#) (required)
- [Configuring an SNMP Context for a VPN, page 37](#) (required)
- [Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2, page 39](#) (required)



## Configuring SNMP Support for a VPN

To configure SNMP support for a VPN (or a remote VPN), perform the following task.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-address* [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
4. **snmp-server engineID remote** *ip-address* [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
5. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server host</b> <i>host-address</i> [ <b>vrf</b> <i>vrf-name</i> ] [ <b>traps</b>   <b>informs</b> ] [ <b>version</b> { <b>1</b>   <b>2c</b>   <b>3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]}] <i>community-string</i> [ <b>udp-port</b> <i>port</i> ] [ <i>notification-type</i> ]  <b>Example:</b> Router(config)# snmp-server host example.com vrf trap-vrf	Specifies the recipient of an SNMP notification operation and specifies the VRF instance table to be used for the sending of SNMP notifications. <ul style="list-style-type: none"> <li>• The <i>host-address</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>• The <b>vrf</b> <i>vrf-name</i> keyword argument pair specifies the VRF table that should be used to send SNMP notifications.</li> <li>• The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>• The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>• The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following:</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>– <b>1</b> —SNMPv1. This option is not available with informs.</li> <li>– <b>2c</b> —SNMPv2C.</li> <li>– <b>3</b> —SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword: <b>auth</b>, <b>noauth</b>, <b>priv</b>.</li> <li>• The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> <li>• The <b>udp-port</b> <i>port</i> keyword argument pair names the UDP port of the host to use. The default is 162.</li> <li>• The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> </ul>
<b>Step 4</b>	<pre>snmp-server engineID remote ip-address [udp-port udp-port-number] [vrf vrf-name] engineid-string</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server engineID remote 172.16.20.3 vrf traps-vrf 80000009030000B064EFE100</pre>	<p>Specifies the SNMP engine ID of a remote SNMP device.</p> <ul style="list-style-type: none"> <li>• The <i>ipv4-address</i> argument is the IPv4 address of the device that contains the remote copy of SNMP.</li> <li>• The <i>ipv6-address</i> argument is the IPv6 address of the device that contains the remote copy of SNMP.</li> <li>• The <b>udp-port</b> keyword specifies a User Datagram Protocol (UDP) port of the host to use.</li> <li>• The <i>udp-port-number</i> argument is the socket number on the remote device that contains the remote copy of SNMP. The default is 161.</li> <li>• The <b>vrf</b> keyword specifies an instance of a routing table.</li> <li>• The <i>vrf-name</i> argument is the name of the VRF table to use for storing data.</li> <li>• The <i>engineid-string</i> is a string of a maximum of 24 characters that identifies the engine ID.</li> </ul>
<b>Step 5</b>	<pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end</pre>	<p>Exits to privileged EXEC mode.</p>

## What to Do Next

Proceed to the [“Configuring an SNMP Context for a VPN”](#) section on page 37.

## Configuring an SNMP Context for a VPN

To configure an SNMP context for a VPN, perform the following task. This sets up a unique SNMP context for a VPN, which allows you to access the VPN’s LDP session information.

### SNMP Context

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN’s specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

### VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables for a VPN. Cisco IOS software adds the RD to the beginning of the customer’s IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

Either the RD is an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter an RD in either of these formats:

- 16-bit ASN: your 32-bit number, for example, 101:3.
- 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server context** *context-name*
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **context** *context-name*
7. **route-target** { **import** | **export** | **both** } *route-target-ext-community*
8. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
	<b>Example:</b> Router> enable	
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>snmp-server context</b> <i>context-name</i>	Creates and names an SNMP context. <ul style="list-style-type: none"> <li>• The <i>context-name</i> argument is the name of the SNMP context being created.</li> </ul>
	<b>Example:</b> Router(config)# snmp-server context context1	

	Command or Action	Purpose
Step 4	<b>ip vrf</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# ip vrf vrf1	Configures a VRF table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>
Step 5	<b>rd</b> <i>route-distinguisher</i>  <b>Example:</b> Router(config-vrf)# rd 100:120	Creates a VPN route distinguisher. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument specifies to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix. You can enter a route distinguisher in either of these formats: <ul style="list-style-type: none"> <li>16-bit autonomous system number: your 32-bit number For example, 101:3.</li> <li>32-bit IP address: your 16-bit number For example, 192.168.122.15:1.</li> </ul> </li> </ul>
Step 6	<b>context</b> <i>context-name</i>  <b>Example:</b> Router(config-vrf)# context context1	Associates an SNMP context with a particular VRF. <ul style="list-style-type: none"> <li>The <i>context-name</i> argument is the name of the SNMP VPN context, up to 32 characters.</li> </ul>
Step 7	<b>route-target</b> { <b>import</b>   <b>export</b>   <b>both</b> } <i>route-target-ext-community</i>  <b>Example:</b> Router(config-vrf)# route-target export 100:1000	(Optional) Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword specifies to import routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword specifies to export routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword specifies to import both import and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul>
Step 8	<b>end</b>  <b>Example:</b> Router(config-vrf)# end	Exits to privileged EXEC mode.

## What to Do Next

Proceed to the [“Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2”](#) section on page 39.

## Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2

To configure a VPN-aware SNMP context for SNMPv1 or SNMPv2, perform the following task. This allows you to access LDP session information for a VPN using SNMPv1 or SNMPv2.

## SNMPv1 or SNMPv2 Security

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP Versions 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP Version 3 performs.

To configure the VPN Aware LDP MIB feature when using SNMP Version 1 or SNMP Version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if they come in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, the packet is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from using a clear text community string to query the VPN data. However, this is not as secure as using SNMPv3.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote host** *[udp-port port]*] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** *access-list*]
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *readview*] [**write** *writeview*] [**notify** *notifyview*] [**access** *access-list*]
5. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
6. **snmp-server enable traps** [*notification-type*]
7. **snmp-server host** *host-address* [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [**notification-type**]
8. **snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] **target-list** *vpn-list-name*
9. **snmp mib target list** *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*}
10. **no snmp-server trap authentication vrf**
11. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
<p><b>Step 3</b></p>	<pre>snmp-server user username group-name [<b>remote</b> host [udp-port port]] {v1   v2c   v3 [encrypted] [auth {md5   sha} auth-password]} [access access-list]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server user customer1 group1 v1</pre>	<p>Configures a new user to an SNMP group.</p> <ul style="list-style-type: none"> <li>• The <i>username</i> argument is the name of the user on the host that connects to the agent.</li> <li>• The <i>group-name</i> argument is the name of the group to which the user belongs.</li> <li>• The <b>remote host</b> keyword and argument specify a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.</li> <li>• The <b>udp-port port</b> keyword and argument specify the UDP port number of the remote host. The default is UDP port 162.</li> <li>• The <b>v1</b> keyword specifies that SNMPv1 should be used.</li> <li>• The <b>v2c</b> keyword specifies that SNMPv2c should be used.</li> <li>• The <b>v3</b> keyword specifies that the SNMPv3 security model should be used. Allows the use of the <b>encrypted</b> and or <b>auth</b> keywords.</li> <li>• The <b>encrypted</b> keyword specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).</li> <li>• The <b>auth</b> keyword specifies which authentication level should be used.</li> <li>• The <b>md5</b> keyword is the HMAC-MD5-96 authentication level.</li> <li>• The <b>sha</b> keyword is the HMAC-SHA-96 authentication level.</li> <li>• The <i>auth-password</i> argument is a string (not to exceed 64 characters) that enables the agent to receive packets from the host. The minimum length for a password is one character. The recommended length of a password is at least eight characters, and should include both letters and numbers.</li> <li>• The <b>access access-list</b> keyword and argument specify an access list to be associated with this SNMP user.</li> </ul>

Command or Action	Purpose
<p><b>Step 4</b></p> <pre>snmp-server group group-name {v1   v2c   v3} {auth   noauth   priv} [context context-name] [read readview] [write writeview] [notify notifyview] [access access-list]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1</pre>	<p>Configures a new SNMP group or a table that maps SNMP users to SNMP views.</p> <ul style="list-style-type: none"> <li>• The <i>group-name</i> argument is the name of the group.</li> <li>• The <b>v1</b> keyword specifies that SNMPv1 should be used for the group.</li> <li>• The <b>v2c</b> keyword specifies that SNMPv2c should be used for the group. The SNMPv2c security model allows for the transmission of informs, and supports 64-character strings (instead of 32-character strings).</li> <li>• The <b>v3</b> keyword specifies that the SNMPv3 should be used for the group. SMNPv3 is the most secure of the supported security models, because it allows you to explicitly configure the authentication characteristics.</li> <li>• The <b>auth</b> keyword specifies authentication of a packet without encrypting it.</li> <li>• The <b>noauth</b> keyword specifies no authentication of a packet.</li> <li>• The <b>priv</b> keyword specifies authentication of a packet with encryption.</li> <li>• The <b>context</b> <i>context-name</i> keyword and argument associate the specified SNMP group with a configured SNMP context.</li> <li>• The <b>read</b> <i>readview</i> keyword and argument specify a read view for the SNMP group. The <i>readview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to display only the contents of the agent.</li> <li>• The <b>write</b> <i>writeview</i> keyword and argument specify a write view for the SNMP group. The <i>writeview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.</li> <li>• The <b>notify</b> and <i>notifyview</i> keyword argument specify a notify view for the SNMP group. The <i>writeview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.</li> <li>• The <b>access</b> <i>access-list</i> keyword and argument specify a standard access list (a standard ACL) to associate with the group.</li> </ul>

	Command or Action	Purpose
Step 5	<pre>snmp-server view view-name oid-tree {included   excluded}</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server view view1 ipForward included</pre>	<p>Creates or updates a view entry.</p> <ul style="list-style-type: none"> <li>The <i>view-name</i> argument is the label for the view record that you are updating or creating. The name is used to reference the record.</li> <li>The <i>oid-tree</i> argument is the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.</li> <li>The <b>included</b> keyword configures the OID (and subtree OIDs) specified in the <i>oid-tree</i> argument to be included in the SNMP view.</li> <li>The <b>excluded</b> keyword configures the OID (and subtree OIDs) specified in the <i>oid-tree</i> argument to be explicitly excluded from the SNMP view.</li> </ul>
Step 6	<pre>snmp-server enable traps [notification-type]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server enable traps</pre>	<p>Enables all SNMP notifications (traps or informs) available on your system.</p> <ul style="list-style-type: none"> <li>The <i>notification-type</i> argument specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host.</li> </ul>
Step 7	<pre>snmp-server host host-address [vrf vrf-name] [traps   informs] [version {1   2c   3 [auth   noauth   priv]] community-string [udp-port port] [notification-type]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server host 10.0.0.1 vrf customer1 public udp-port 7002</pre>	<p>Specifies the recipient of an SNMP notification operation.</p> <ul style="list-style-type: none"> <li>The <i>host-address</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword argument pair specifies the VRF table that should be used to send SNMP notifications.</li> <li>The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following: <ul style="list-style-type: none"> <li><b>1</b> —SNMPv1. This option is not available with informs.</li> <li><b>2c</b> —SNMPv2C.</li> <li><b>3</b> —SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword: <b>auth</b>, <b>noauth</b>, <b>priv</b>.</li> </ul> </li> </ul>



Command or Action	Purpose
	<ul style="list-style-type: none"> <li>The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> <li>The <b>udp-port</b> <i>port</i> keyword argument pair names the UDP port of the host to use. The default is 162.</li> <li>The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> </ul>
<p><b>Step 8</b></p> <pre>snmp mib community-map community-name [context context-name] [engineid engine-id] [security-name security-name] target-list vpn-list-name</pre> <p><b>Example:</b>  Router(config)# snmp mib community-map community1 context context1 target-list commAVpn</p>	<p>Associates an SNMP community with an SNMP context, engine ID, or security name.</p> <ul style="list-style-type: none"> <li>The <i>community-name</i> argument is an SNMP community string.</li> <li>The <b>context</b> <i>context-name</i> keyword and argument specify an SNMP context name to be mapped to the SNMP community.</li> <li>The <b>engineid</b> <i>engine-id</i> keyword and argument specify an SNMP engine ID to be mapped to the SNMP community.</li> <li>The <b>security-name</b> <i>security-name</i> keyword and argument specify the security name to be mapped to the SNMP community.</li> <li>The <b>target-list</b> <i>vpn-list-name</i> keyword and argument specify the VRF list to be mapped to the SNMP community. The list name should correspond to a list name used in the <b>snmp mib target list</b> command.</li> </ul>
<p><b>Step 9</b></p> <pre>snmp mib target list vpn-list-name {vrf vrf-name   host ip-address}</pre> <p><b>Example:</b>  Router(config)# snmp mib target list commAVpn vrf vrf1</p>	<p>Creates a list of target VRFs and hosts to associate with an SNMP community.</p> <ul style="list-style-type: none"> <li>The <i>vpn-list-name</i> argument is the name of the target list.</li> <li>The <b>vrf</b> keyword adds a specified VRF to the target list.</li> <li>The <i>vrf-name</i> argument is the name of a VRF to include in the list.</li> <li>The <b>host</b> keyword adds a specified host to the target list.</li> <li>The <i>ip-address</i> argument is the IP address of the host.</li> </ul>
<p><b>Step 10</b></p> <pre>no snmp-server trap authentication vrf</pre> <p><b>Example:</b>  Router(config)# no snmp-server trap authentication vrf</p>	<p>(Optional) Disables all SNMP authentication notifications (traps and informs) generated for packets received on VRF interfaces.</p> <ul style="list-style-type: none"> <li>Use this command to disable authentication traps only for those packets on VRF interfaces with incorrect community associations.</li> </ul>
<p><b>Step 11</b></p> <pre>end</pre> <p><b>Example:</b>  Router(config) end</p>	<p>Exits to privileged EXEC mode.</p>

# Configuration Examples for MPLS EM—MPLS LDP MIB - RFC 3815

This section contains the following configuration examples for MPLS EM—MPLS LDP MIB-RFC 3815:

- [Configuring Access to an SNMP Agent on a Host NMS Workstation: Example, page 45](#)
- [Configuring the Router to Send SNMP Notifications to a Host for Monitoring LDP: Example, page 45](#)
- [Configuring a VPN-Aware LDP MIB: Example, page 46](#)

## Configuring Access to an SNMP Agent on a Host NMS Workstation: Example

The following example shows how to configure access to an SNMP agent on a host NMS workstation:

```
configure terminal
!
snmp-server community
end
```

The following example shows how to configure access to SNMPv1 and SNMPv2C on the host NMS workstation. The configuration permits any SNMP agent to access all MPLS LDP MIB objects with read-only permission using the community string public.

```
configure terminal
!
snmp-server community public
end
```

The following example shows how to allow read-only access to all MPLS LDP MIB objects relating to members of access list 4 that specify the comaccess community string. No other SNMP agents will have access to any of the MPLS LDP MIB objects.

```
configure terminal
!
snmp-server community comaccess ro 4
end
```

## Configuring the Router to Send SNMP Notifications to a Host for Monitoring LDP: Example

The following example shows how to configure the router to send SNMP notifications to a host for monitoring LDP:

```
config terminal
!
snmp-server host 172.20.2.160 traps comaccess mpls-ldp
snmp-server enable traps mpls rfc ldp session-up
!
snmp-server enable traps mpls rfc ldp session-down
end
```

The session up and session down LDP notifications are configured.

## Configuring a VPN-Aware LDP MIB: Example

This section contains the following examples for configuring a VPN-aware LDP MIB:

- [Configuring SNMP Support for a VPN: Example, page 46](#)
- [Configuring an SNMP Context for a VPN: Example, page 46](#)
- [Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2: Example, page 46](#)

### Configuring SNMP Support for a VPN: Example

The following example shows how to configure SNMP support for a VPN:

```
configure terminal
!
snmp-server host 10.10.10.1 vrf traps-vrf
snmp-server engineID remote 172.16.20.3 vrf traps-vrf 80000009030000B064EFE100
end
```

### Configuring an SNMP Context for a VPN: Example

The following example shows how to configure an SNMP context for a VPN. In this example, the VPN vrf1 is associated with the SNMP context context1.

```
configure terminal
!
snmp-server context context1
ip vrf vrf1
rd 100:120
context context1
route-target export 100:1000
end
```

### Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2: Example

The following configuration example shows how to configure a VPN-aware SNMP context for the MPLS LDP MIB with SNMPv1 or SNMPv2:

```
snmp-server context A
snmp-server context B

ip vrf CustomerA
rd 100:110
context A
route-target export 100:1000
route-target import 100:1000
!

ip vrf CustomerB
rd 100:120
context B
route-target export 100:2000
route-target import 100:2000
!

interface Ethernet3/1
description Belongs to VPN A
ip vrf forwarding CustomerA
ip address 10.0.0.0 255.255.0.0
```

```

interface Ethernet3/2
  description Belongs to VPN B
  ip vrf forwarding CustomerB
  ip address 10.0.0.1 255.255.0.0

snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c

snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB

snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included

snmp-server enable traps
snmp-server host 10.0.0.3 vrf CustomerA commA udp-port 7002
snmp-server host 10.0.0.4 vrf CustomerB commB udp-port 7002

snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid

```

## Additional References

The following sections provide references related to the MPLS EM—MPLS LDP MIB - RFC 3815 feature.

## Related Documents

Related Topic	Document Title
MPLS LDP concepts and configuration tasks	<a href="#">MPLS Label Distribution Protocol</a> ” chapter in the <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i>
A description of SNMP agent support in the Cisco IOS software for the MPLS Label Switching Router MIB (MPLS-LSR-STD-MIB)	<a href="#">MPLS EM—MPLS LSR MIB - RFC 3813</a>
SNMP commands	<a href="#">Cisco IOS Network Management Command Reference</a>
SNMP configuration	“Configuring SNMP Support” chapter in the <i>Cisco IOS Network Management Configuration Guide</i>
SNMP support for VPNs	<a href="#">SNMP Notification Support for VPNs</a>
SNMP context support for VPNs configuration tasks	<a href="#">SNMP Support over VPNs—Context Based Access Control</a>
MPLS concepts and configuration tasks	<a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a>

## Additional References

Related Topic	Document Title
CEF concepts and configuration tasks	“Configuring Cisco Express Forwarding” section in the <i>Cisco IOS IP Switching Configuration Guide</i>
Information about MPLS EM	<i>Cisco IOS MPLS Embedded Management Application Note</i> <i>Cisco IOS MPLS Embedded Management Q&amp;A</i>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>MPLS-LDP-STD-MIB</li> <li>MPLS-LDP-ATM-STD-MIB</li> <li>MPLS-LDP-FRAME-RELAY-STD-MIB</li> <li>MPLS-LDP-GENERIC-STD-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS s, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 3036	<i>LDP Specification</i>
RFC 3037	<i>LDP Applicability</i>
RFC 3815	<i>Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **snmp-server enable traps mpls rfc ldp**

# Feature Information for MPLS EM—MPLS LDP MIB - RFC 3815

Table 20 lists the history for this feature.

Not all commands may be available in your Cisco IOS software. For information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 20 lists only the Cisco IOS software that introduced support for a given feature in a given Cisco IOS software train. Unless noted otherwise, subsequent releases of that Cisco IOS software train also support that feature.

**Table 20** Feature Information for MPLS EM—MPLS LDP MIB - RFC 3815

Feature Name	Releases	Feature Information
MPLS EM—MPLS LDP MIB - RFC 3815	12.2(33)SRB 12.2(33)SB	<p>The MPLS EM—MPLS LDP MIB - RFC 3815 feature document describes the MIBs that support the Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) based on RFC 3815, <i>Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)</i>, and describes the differences between RFC 3815 and the MPLS-LDP-MIB based on the Internet Engineering Task Force (IETF) draft Version 8 (draft-ietf-mpls-ldp-08.txt). RFC 3815 and IETF draft Version 8 provide an interface for managing LDP through the use of the Simple Network Management Protocol (SNMP).</p> <p>In RFC 3815, the content of the MPLS-LDP-MIB is divided into four MIB modules: the MPLS-LDP-STD-MIB, the MPLS-LDP-GENERIC-STD-MIB, the MPLS-LDP-ATM-STD-MIB, and the MPLS-LDP-FRAME-RELAY-STD-MIB.</p> <p>Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.</p> <p>In 12.2(33)SRB, this feature was introduced.</p> <p>In 12.2(33)SB, the feature was integrated into Cisco IOS Release 12.2SB.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Label Distribution Protocol Overview, page 3</a></li> </ul>

**Table 20**      *Feature Information for MPLS EM—MPLS LDP MIB - RFC 3815 (continued)*

Feature Name	Releases	Feature Information
		<ul style="list-style-type: none"> <li>• <a href="#">Benefits of Using the MPLS EM—MPLS LDP MIB - RFC 3815 Feature</a>, page 5</li> <li>• <a href="#">MPLS LDP MIB (RFC 3815) Elements</a>, page 6</li> <li>• <a href="#">Events Generating MPLS LDP MIB Notifications</a>, page 10</li> <li>• <a href="#">Scalar Objects in the MPLS LDP MIB Modules (RFC 3815)</a>, page 11</li> <li>• <a href="#">MIB Tables in the MPLS-LDP-STD-MIB Module (RFC 3815)</a>, page 12</li> <li>• <a href="#">MIB Tables in the MPLS-LDP-ATM-STD-MIB Module (RFC 3815)</a>, page 19</li> <li>• <a href="#">MIB Table in the MPLS-LDP-GENERIC-STD-MIB Module (RFC 3815)</a>, page 21</li> <li>• <a href="#">VPN Contexts in the MPLS LDP MIB</a>, page 22</li> <li>• <a href="#">Differences Between the MPLS-LDP-STD-MIB and the MPLS-LDP-MIB</a>, page 25</li> <li>• <a href="#">Differences Between the MPLS-LDP-MIB and the MPLS-LDP-ATM-STD-MIB (RFC 3815)</a>, page 30</li> <li>• <a href="#">Differences Between the MPLS-LDP-MIB and the MPLS-LDP-GENERIC-STD-MIB (RFC 3815)</a>, page 31</li> <li>• <a href="#">Differences Between the MPLS-LDP-MIB and the MPLS-LDP-GENERIC-STD-MIB (RFC 3815)</a>, page 31</li> <li>• <a href="#">Configuring Access to an SNMP Agent on a Host NMS Workstation</a>, page 31</li> <li>• <a href="#">Configuring the Router to Send SNMP Notifications to a Host for Monitoring LDP</a>, page 33</li> <li>• <a href="#">Configuring a VPN-Aware LDP MIB</a>, page 35</li> <li>• <a href="#">Configuring a VPN-Aware LDP MIB</a>, page 35</li> </ul> <p>The following command was introduced in this feature:  <b>snmp-server enable traps mpls rfc ldp.</b></p>



# Glossary

**FPI**—forwarding path identifier. An identifier required to locate Multiprotocol Label Switching (MPLS) forwarding information for a forwarding equivalence class (FEC). Examples of types of FPIs supported by the MPLS Forwarding Infrastructure (MFI) are IPv4, IPv6, LABEL, SSS, and TE.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

**LFIB**—Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSP**—label switched path. A sequence of hops in which a packet travels from one router to another router by means of label switching mechanisms. A label switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

**LSR**—label switch router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MFI**—MPLS Forwarding Infrastructure. In the Cisco MPLS subsystem, the data structure for storing information about incoming and outgoing labels and associated equivalent packets suitable for labeling.

**MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MOI**—MPLS output information. The MOI includes the next hop, outgoing interface, and outgoing label.

**MPLS**—Multiprotocol Label Switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**NMS**—network management station. A device (usually a workstation) that performs Simple Network Management Protocol (SNMP) queries to the SNMP agent of a managed device to retrieve or modify information.

**notification request**—Message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. SNMP notification requests are more reliable than traps, because a notification request from an SNMP agent requires that the SNMP manager acknowledge receipt of the notification request. The manager replies with an SNMP response protocol data unit (PDU). If the manager does not receive a notification message from an SNMP agent, it does not send a response. If the sender (SNMP agent) never receives a response, the notification request can be sent again. Thus, a notification request is more likely than a trap to reach its intended destination.

**SNMP**—Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**trap**—Message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

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

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2007–2009 Cisco Systems, Inc. All rights reserved.





# MPLS EM—MPLS LSR MIB - RFC 3813

---

**First Published: February 19, 2007**

**Last Updated: April 11, 2008**

The MPLS LSR MIB- RFC 3813 (MPLS-LSR-STD-MIB) allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switch router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology.

This document describes the MPLS-LSR-STD-MIB. The document also describes the major differences between the MPLS-LSR-STD-MIB and draft Version 5 of the MPLS-LSR-MIB.

The MPLS EM—MPLS LSR MIB - RFC 3813 feature introduces the MPLS-LSR-STD-MIB, which is an upgrade from draft Version 5 of the MPLS-LSR-MIB to an implementation of the *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)*, RFC 3813. This feature also introduces the VPN Aware LSR MIB feature that enables the MPLS-LSR-STD-MIB to get VPN context information.

Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for MPLS EM—MPLS LSR MIB - RFC 3813](#)” section on [page 39](#).

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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



---

**Americas Headquarters:**

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

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

# Contents

- [Prerequisites for MPLS EM—MPLS LSR MIB - RFC 3813, page 2](#)
- [Information About MPLS EM—MPLS LSR MIB - RFC 3813, page 3](#)
- [How to Configure SNMP for the MPLS EM—MPLS LSR MIB - RFC 3813, page 23](#)
- [Configuration Examples for the MPLS EM—MPLS LSR MIB - RFC 3813, page 35](#)
- [Additional References, page 37](#)
- [Command Reference, page 38](#)
- [Feature Information for MPLS EM—MPLS LSR MIB - RFC 3813, page 39](#)
- [Glossary, page 41](#)

## Prerequisites for MPLS EM—MPLS LSR MIB - RFC 3813

The MPLS-LSR-STD-MIB requires the following:

- SNMP installed and enabled on the LSR
- MPLS enabled on the LSR
- MPLS Forwarding Infrastructure (MFI)

## Restrictions for MPLS EM—MPLS LSR MIB - RFC 3813

- The implementation of the MPLS-LSR-STD-MIB (RFC 3815) for Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB is limited to read-only (RO) permission for MIB objects.
- The following MIB objects are not supported in Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB:
  - mplsInterfaceTotalBandwidth (MPLS interface table)
  - mplsInterfaceAvailableBandwidth (MPLS interface table)
  - mplsInterfacePerfInLabelLookupFailures (MPLS interface performance table)
  - mplsInterfacePerfOutFragmentedPkts (MPLS interface performance table)
  - mplsInSegmentTrafficParamPtr (MPLS in-segment table)
  - mplsInSegmentPerfDiscards (MPLS in-segment performance table)
- The following notifications are not supported:
  - mplsXCUp
  - mplsXCDown

# Information About MPLS EM—MPLS LSR MIB - RFC 3813

Before you configure SNMP and the MPLS-LSR-STD-MIB to remotely manage an MPLS LSR, you should understand the following concepts:

- [MPLS-LSR-STD-MIB Benefits, page 3](#)
- [Label Switching Information Managed by the MPLS-LSR-STD-MIB, page 4](#)
- [MPLS-LSR-STD-MIB Elements, page 5](#)
- [Brief Description of MPLS-LSR-STD-MIB Tables, page 5](#)
- [MPLS LSR Information Available Through the MPLS-LSR-STD-MIB, page 5](#)
- [Information from MPLS-LSR-STD-MIB Scalar Objects, page 10](#)
- [MPLS-LSR-STD-MIB Indexing—Linking Table Elements, page 11](#)
- [Interface Configuration Table and Interface MIB Links, page 12](#)
- [MPLS-LSR-STD-MIB Structure, page 13](#)
- [CLI Commands and the MPLS-LSR-MIB, page 14](#)
- [VPN Aware LSR MIB, page 16](#)
- [Major Differences Between the MPLS-LSR-STD-MIB and the MPLS-LSR-MIB, page 17](#)

## MPLS-LSR-STD-MIB Benefits

The benefits described in the following paragraphs are available to you with the MPLS-LSR-STD-MIB.

### LSR Problem Troubleshooting

By monitoring the cross-connect entries and the associated incoming and outgoing segments, you can see which labels are installed and how they are being swapped. Use the MPLS-LSR-STD-MIB in place of the **show mpls forwarding** command-line interface (CLI) command.

### LSR Traffic Load Monitoring

By monitoring interface and packet operations on an MPLS LSR, you can identify high- and low-traffic patterns, and traffic distributions.

### Improvement of Network Performance

By identifying potentially high-traffic areas, you can set up load sharing to improve network performance.

### Verification of LSR Configuration

By comparing results from SNMP **get** commands and the **show mpls forwarding** CLI command, you can verify your LSR configuration.

### Active Label Switched Paths Monitoring

By monitoring the cross-connect entries and the associated incoming segments and outgoing segments, you can determine the active LSPs.

## Label Switching Information Managed by the MPLS-LSR-STD-MIB

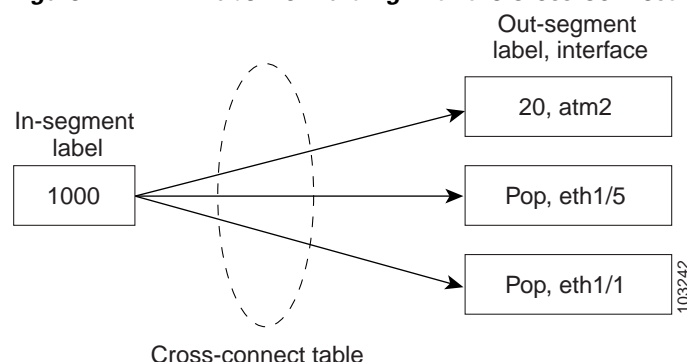
The MPLS-LSR-STD-MIB contains managed objects that support the retrieval of label switching information from a router. The MIB is based on RFC 3813. This implementation enables a network administrator to get information on the status, character, and performance of the following:

- MPLS-capable interfaces on the LSR
- Incoming MPLS segments (labels) at an LSR and their associated parameters
- Outgoing segments (labels) at an LSR and their associated parameters

In addition, the network administrator can retrieve the status of cross-connect table entries that associate MPLS segments with each other.

Figure 1 shows the association of the cross-connect table with incoming and outgoing segments (labels).

**Figure 1** Label Forwarding with the Cross-Connect Table



### Note

The out-segment table does not display “no label” entries. Labels that are displayed as “POP” are the special MPLS label 3.

The notation used in the MPLS-LSR-STD-MIB follows the conventions defined in Abstract System Notation One (ASN.1). ASN.1 defines an Open Systems Interconnection (OSI) language used to describe data types independently from particular computer structures and presentation techniques. Each object in the MIB incorporates a DESCRIPTION field that includes an explanation of the object’s meaning and usage, which, together with the other characteristics of the object (SYNTAX, MAX-ACCESS, and INDEX) provides sufficient information for management application development, as well as for documentation and testing.

The MPLS-LSR-STD-MIB represents an ASN.1 notation that represents an idealized MPLS LSR.

A network administrator can access the entries (objects) in the MPLS-LSR-STD-MIB by means of any SNMP-based network management system (NMS). The network administrator can retrieve information in the MPLS-LSR-STD-MIB using standard SNMP **get** and **getnext** commands.

Typically, SNMP runs as a low-priority process. The response time for the MPLS-LSR-STD-MIB is expected to be similar to that for other MIBs. The size and structure of the MIB and other MIBs in the system influence response time when you retrieve information from the management database. Traffic through the LSR also affects SNMP performance. The busier the switch is with forwarding activities, the greater the possibility of lower SNMP performance.

## MPLS-LSR-STD-MIB Elements

The top-level components of the MPLS-LSR-STD-MIB are:

- Tables and scalars (mplsLsrObjects)
- Notifications (mplsLsrNotifications)
- Conformance (mplsLsrConformance)

## Brief Description of MPLS-LSR-STD-MIB Tables

This section lists and briefly describes of the main and supplementary tables in the MPLS-LSR-STD-MIB.

The Cisco implementation of the MPLS-LSR-STD-MIB supports four main tables:

- MPLS interface table (mplsInterfaceTable)—Contains entries for all MPLS-capable interfaces on the LSR.
- MPLS in-segment table (mplsInSegmentTable)—Contains a description of incoming labels on the LSR.
- Mpls out-segment table (mplsOutSegmentTable)—Contains a description of outgoing labels on the LSR.
- MPLS cross-connect table (mplsXCTable)—Contains the connections between the in-segments and out-segments on the LSR. A single cross-connect entry is equivalent to a single entry in the Label Forwarding Information Base (LFIB), showing an in-label being switched to an out-label. A cross-connect entry can exist where no corresponding in-segment exists. For example, only the outgoing label exists at the head end of a traffic engineering (TE) tunnel.

Three tables manage labels, the MPLS in-segment table, the MPLS out-segment table, and the MPLS cross-connect tables.

The MIB contains three supplementary tables to supply performance information:

- MPLS interface performance table (mplsInterfacePerfTable)—Augments the MPLS interface table. Provides objects to measure performance for MPLS-capable interfaces on the LSR.
- MPLS in-segment performance table (mplsInSegmentPerfTable)—Augments the MPLS in-segment table. Provides performance information and counters for incoming segments on the LSR.
- MPLS out-segment performance table (mplsOutSegmentPerfTable)—Augments the MPLS out-segment table. Provides performance information and counters for outgoing segments on the LSR.

## MPLS LSR Information Available Through the MPLS-LSR-STD-MIB

You can use SNMP **get** and **getnext** commands to gather label switching information for an MPLS LSR available through the MPLS-LSR-STD-MIB tables. This section describes the MPLS LSR information available from each table:

- [MPLS Interface Table \(mplsInterfaceTable\)](#), page 6
- [MPLS Interface Performance Table \(mplsInterfacePerfTable\)](#), page 6
- [MPLS In-Segment Table \(mplsInSegmentTable\)](#), page 7
- [MPLS In-Segment Performance Table \(mplsInSegmentPerfTable\)](#), page 7



- [MPLS Out-Segment Table \(mplsOutSegmentTable\)](#), page 8
- [MPLS Out-Segment Performance Table \(mplsOutSegmentPerfTable\)](#), page 9
- [MPLS Cross-Connect Table \(mplsXCTable\)](#), page 9
- [MPLS Label Stack Table \(mplsLabelStackTable\)](#), page 10
- [MPLS In-Segment Map Table \(mplsInSegmentMapTable\)](#), page 10

## MPLS Interface Table (mplsInterfaceTable)

[Table 1](#) lists the MPLS LSR information and associated MIB objects provided by the MPLS interface table (mplsInterfaceTable).

**Table 1** *MPLS Interface Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Minimum value for an MPLS label that can be received on the interface	<code>mplsInterfaceLabelMinIn</code>
Maximum value for an MPLS label that can be received on the interface	<code>mplsInterfaceLabelMaxIn</code>
A unique MPLS-enabled interface index or 0	<code>mplsInterfaceIndex</code>
Minimum value for an MPLS label that the LSR can send from the interface	<code>mplsInterfaceLabelMinOut</code>
Maximum value for an MPLS label that the LSR can send from the interface	<code>mplsInterfaceLabelMaxOut</code>
Per platform (0) or per interface (1) setting	<code>mplsInterfaceLabelParticipationType</code>

The following MIB objects and associated MPLS LSR information from the MPLS interface table are not supported:

- `mplsInterfaceTotalBandwidth`—The total usable bandwidth on the interface.
- `mplsInterfaceAvailableBandwidth`—The difference between the total usable bandwidth and the bandwidth in use.

## MPLS Interface Performance Table (mplsInterfacePerfTable)

[Table 2](#) lists the MPLS LSR information and associated MIB objects provided by the MPLS interface performance table (mplsInterfacePerfTable).

**Table 2** *MPLS Interface Performance Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Number of labels in the incoming direction in use	<code>mplsInterfacePerfInLabelsInUse</code>
Number of top-most labels in outgoing label stacks in use	<code>mplsInterfacePerfOutLabelsInUse</code>

The following MIB objects and associated MPLS LSR information from the MPLS interface performance table are not supported:

- `mplsInterfacePerfInLabelLookupFailures`—The number of labeled packets discarded because no cross-connect entries exist.
- `mplsInterfacePerfOutFragmentedPkts`—The number of outgoing MPLS packets requiring fragmentation for transmission.

## MPLS In-Segment Table (`mplsInSegmentTable`)

Table 3 lists the MPLS LSR information and associated MIB objects provided by the MPLS in-segment table (`mplsInSegmentTable`).

**Table 3** *MPLS In-Segment Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Unique index identifier	<code>mplsInSegmentIndex</code>
Interface index for the incoming MPLS interface	<code>mplsInSegmentInterface</code>
Incoming label	<code>mplsInSegmentLabel</code>
Pointer to an external table containing the label, if not represented fully in the <code>mplsInSegmentLabel</code> object	<code>mplsInSegmentLabelPtr</code>
Number of labels to pop (remove) from the incoming segment	<code>mplsInSegmentNPop</code>
An address family number from the Internet Assigned Number Authority (IANA)	<code>mplsInSegmentAddrFamily</code>
Segment cross-connect entry association	<code>mplsInSegmentXCIndex</code>
Segment owner	<code>mplsInSegmentOwner</code>
Status of the table row	<code>mplsInSegmentRowStatus</code>
Storage type	<code>mplsInSegmentStorageType</code>

The following MIB object and associated MPLS LSR information from the MPLS in-segment table is not supported:

- `mplsInSegmentTrafficParamPtr`—A pointer to a traffic parameter table entry (set to the default 0.0).

## MPLS In-Segment Performance Table (`mplsInSegmentPerfTable`)

Table 4 lists the MPLS LSR information and associated MIB objects provided by the MPLS in-segment performance table (`mplsInSegmentPerfTable`).

**Table 4** *MPLS In-Segment Performance Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Number of 32-bit octets received	<code>mplsInSegmentPerfOctets</code>
Number of 64-bit octets received	<code>mplsInSegmentPerfHOctets</code>
Total number of packets received	<code>mplsInSegmentPerfPackets</code>

**Table 4** *MPLS In-Segment Performance Table—MPLS LSR Information and Associated MIB Object (continued)*

MPLS LSR Information	MIB Object
Number of packets with errors	mplsInSdegmentPerfErrors
Time of the last system failure that corresponded to one or more incoming segment discontinuities	mplsInSegmentPerfDiscontinuityTime

The following MIB object and associated MPLS LSR information from the MPLS in-segment performance table is not supported:

- mplsInSegmentPerfDiscards—The number of labeled packets discarded with no errors.

## MPLS Out-Segment Table (mplsOutSegmentTable)

Table 5 lists the MPLS LSR information and associated MIB objects provided by the MPLS out-segment table (mplsOutSegmentTable).

**Table 5** *MPLS Out-Segment Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Unique index identifier	mplsOutSegmentIndex
Interface index of the outgoing interface	mplsOutSegmentInterface
Indication of whether a top label is pushed onto the outgoing packet's label stack	mplsOutSegmentPushToptLabel
Label to push onto the outgoing packet's label stack (if the mplsOutSegmentPushToptLabel is true)	mplsOutSegmentToptLabel
Pointer to an external table containing the label, if not represented fully in the mplsOutSegmentTopLabel object (set to the default 0.0)	mplsOutSegmentTopLabelPtr
Next-hop Internet address type (unknown [0], ipv4 [1], ipv6 [2])	mplsOutSegmentNextHopAddrType
Internet address of the next hop	mplsOutSegmentNextHopAddr
Segment cross-connect entry association	mplsOutSegmentXCIndex
Segment owner	mplsOutSegmentOwner
Status of the table row	mplsOutSegmentRowStatus
Storage type	mplsOutSegmentStorageType

The following MIB object and associated MPLS LSR information from the8—A pointer to a traffic parameter table entry (set to the default 0.0).

## MPLS Out-Segment Performance Table (mplsOutSegmentPerfTable)

Table 6 lists the MPLS LSR information and associated MIB objects provided by the MPLS out-segment performance table (mplsOutSegmentPerfTable).

**Table 6** *MPLS Out-Segment Performance Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Number of 32-bit octets sent	mplsOutSegmentPerfOctets
Total number of packets sent	mplsOutSegmentPerfPackets
Number of packets that could not be sent because of errors	mplsOutSegmentPerfErrors
Number of 64-bit octets sent	mplsOutSegmentPerfHOctets
The time of the last system failure that corresponded to one or more outgoing segment discontinuities	mplsOutSegmentPerfDiscontinuityTime

The following MIB object and associated MPLS LSR information from the MPLS out-segment performance table is not supported:

- mplsOutSegmentPerfDiscards—The number of packets discarded with no errors.

## MPLS Cross-Connect Table (mplsXCTable)

Table 7 lists the MPLS LSR information and associated MIB objects provided by the MPLS cross-connect table (mplsXCTable).

**Table 7** *MPLS Cross-Connect Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Unique index identifier for a group of cross-connect segments	mplsXCIndex
In-segment label index	mplsXCInSegmentIndex
Out-segment index	mplsXCOutSegmentIndex
Label switched path (LSP) to which the cross-connect entry belongs	mplsXCLspId
Index to the MPLS label stack table that identifies the stack of labels to be pushed under the top label	mplsXCLabelStackIndex
Cross-connect owner	mplsXCOwner
Status of table row	mplsXCRowStatus
Storage type	mplsXCStorageType
Administrative status (if up)	mplsXCAdminStatus
Operational status (if up)	mplsXCOperStatus

**Note**

The administrative status and operational status are always up in the Cisco implementation. Otherwise, these status entries do not appear in the table.

## MPLS Label Stack Table (mplsLabelStackTable)

Table 8 lists the MPLS LSR information and associated MIB objects provided by the MPLS label stack table (mplsLabelStackTable).

**Table 8** *MPLS Label Stack Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Primary index for a stack of labels to be pushed on an outgoing packet	mplsLabelStackIndex
Secondary index identifying one label of the stack	mplsLabelStackLabelIndex
Label to be pushed	mplsLabelStackLabel
Pointer to an external table containing the label, if not represented fully in the mplsLabelStackLabel object	mplsLabelStackLabelPtr
Status of the table row	mplsLabelStackRowStatus
Storage type	mplsLabelStackStorageType

## MPLS In-Segment Map Table (mplsInSegmentMapTable)

Table 9 lists the MPLS LSR information and associated MIB objects provided by the MPLS in-segment map table.

**Table 9** *MPLS In-Segment Map Table—MPLS LSR Information and Associated MIB Object*

MPLS LSR Information	MIB Object
Index containing the same value as the mplsInSegmentInterface in the MPLS in-segment table	mplsInSegmentMapInterface
Index containing the same value as the mplsInSegmentLabel in the MPLS in-segment table	mplsInSegmentMapLabel
Pointer to an external table containing the label, if the label for the in-segment cannot be represented fully in the mplsInSegmentLabel object	mplsInSegmentMapLabelPtrIndex
The mplsInSegmentIndex that corresponds to the mplsInSegmentInterface and mplsInSegmentLabel objects or the mplsInSegmentInterface and mplsInSegmentLabelPtr objects	mplsInSegmentMapIndex

## Information from MPLS-LSR-STD-MIB Scalar Objects

The MPLS-LSR-STD-MIB supports several scalar objects. In the Cisco implementation of the MIB for Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB, the following scalar objects are hard-coded to the value indicated and are read-only objects. This symbol (“ ”) indicates an empty string.

- `mplsInSegmentIndexNext` (“ ”)—The value for the in-segment index when the LSR creates an entry in the MPLS in-segment table. The “ ” indicates that this is not implemented because modifications to this table are not allowed.
- `mplsOutSegmentIndexNext` (“ ”)—The value for the out-segment index when an LSR creates a new entry in the MPLS out-segment table. The “ ” indicates that this is not implemented because modifications to this table are not allowed.
- `mplsXCIndexNext` (“ ”)—The value for the cross-connect index when an LSR creates an entry in the MPLS cross-connect table. The “ ” indicates that no unassigned values are available.
- `mplsMaxLabelStackDepth` (6)—The value for the maximum stack depth.
- `mplsLabelStackIndexNext` (“ ”)—The value for the label stack index when an LSR creates entries in the MPLS label stack table. The “ ” indicates that no unassigned values are available.
- `mplsXCNotificationEnable` (false)—Cross-connect notifications are not sent when this value is false.

The following notifications are not supported:

- `mplsXCUp`
- `mplsXCDown`

## MPLS-LSR-STD-MIB Indexing—Linking Table Elements

In the MPLS cross-connect table, cross-connect entries associate incoming segments with outgoing segments. The following objects index the cross-connect entry:

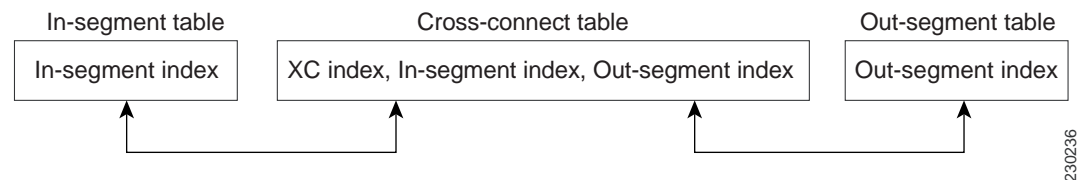
- Cross-connect index (`mplsXCIndex`)—A unique identifier for a group of cross-connect entries in the cross-connect table.
- In-segment index (`mplsXCInSegmentIndex`)—The value of this object is the same value as for the `mplsInSegmentIndex` in the in-segment table.

The in-segment table (`mplsInSegmentTable`) is indexed by the incoming label. The `mplsInSegmentIndex` is a 4-byte octet string containing the local label.

- Out-segment index (`mplsXCOutSegmentIndex`)—The value of this object is the same value as for the `mplsOutSegmentIndex` in the out-segment table.

The following figure shows the relationship among the indexes of the `mplsInSegmentTable`, the `mplsXCTable`, and the `mplsOutSegmentTable`.

**Figure 2** *MPLS-LSR-STD-MIB Indexing*



The `mplsInSegmentIndex`, `mplsXCIndex`, and `mplsOutSegmentIndex` values are defined as an `MplsIndexType`, which is a variable-length octet string that can be used to specify an interface index, a physical card or device, or an application ID.

**MPLS In-Segment Table Index**

The `mplsInSegmentIndex` is a 4-byte octet string containing the local label.

**MPLS Cross-Connect Table Index**

The `mplsXCIndex` is a variable-length octet string, the size of which depends on the application type that is represented and the amount of information needed to represent the label for that application type. The application type is based on a forwarding path identifier (FPI) type that is supported by the MFI. The Cisco implementation of the MPLS-LSR-STD-MIB for Cisco IOS Release xx.x(x)X supports the following FPI types: LABEL, TE, and IPv4.

Figure 3 shows how the MPLS-LSR-STD-MIB represents the application types for the cross-connect `mplsXCIndex` object.

**Figure 3** MPLS-LSR-STD-MIB Application Type Representation for `mplsXCIndex` Object

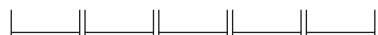
**Legend:**

□ = 1 Byte

FPI - refers to the forwarding path identifier type

LABEL (Length = 5 Bytes) (FPI = 0):

<-FPI-><-----Label----->



TE (Length = 5 Bytes) (FPI = 1):

<-FPI-><-----TE id ----->



IPv4 (Length = 6 Bytes) (FPI = 2):

<-FPI-><-----Prefix-----><mask->



230237

**MPLS Out-Segment Table Index**

The `mplsOutSegmentIndex` is a variable-length octet string. The description of this index is identical to that of the `mplsXCIndex` except the `mplsOutSegmentIndex` is two bytes longer in length. The last two bytes in the out-segment index contains the MPLS output information (MOI) list index.

## Interface Configuration Table and Interface MIB Links

The MPLS interface configuration table lists interfaces that support MPLS technology. An LSR creates an entry dynamically in this table for each MPLS-capable interface. An interface becomes MPLS-capable when MPLS is enabled on that interface. A nonzero index for an entry in this table points to the `ifIndex` for the corresponding interface entry in the MPLS-layer in the `ifTable` of the Interfaces Group MIB.

The `ifTable` contains information on each interface in the network. Its definition of an interface includes any sublayers of the internetwork layer of the interface. MPLS interfaces fit into this definition of an interface. Therefore, each MPLS-enabled interface is represented by an entry in the `ifTable`.

The interrelation of entries in the ifTable is defined by the interfaces stack group of the Interfaces Group MIB. [Figure 4](#) shows how the stack table might appear for MPLS interfaces. The underlying layer refers to any interface that is defined for MPLS internetworking, for example, ATM, Frame Relay, or Ethernet.

**Figure 4** Interface Group MIB Stack Table for MPLS Interfaces

MPLS-interface ifType = mpls(166)	51273
Underlying Layer . . .	



**Note**

Tunnel interfaces are included in the MPLS list for the current implementation.

## MPLS-LSR-STD-MIB Structure

MIB structure is represented by a tree hierarchy. Branches along the tree have short text strings and integers to identify them. Text strings describe object names, and integers allow computer software to encode compact representations of the names.

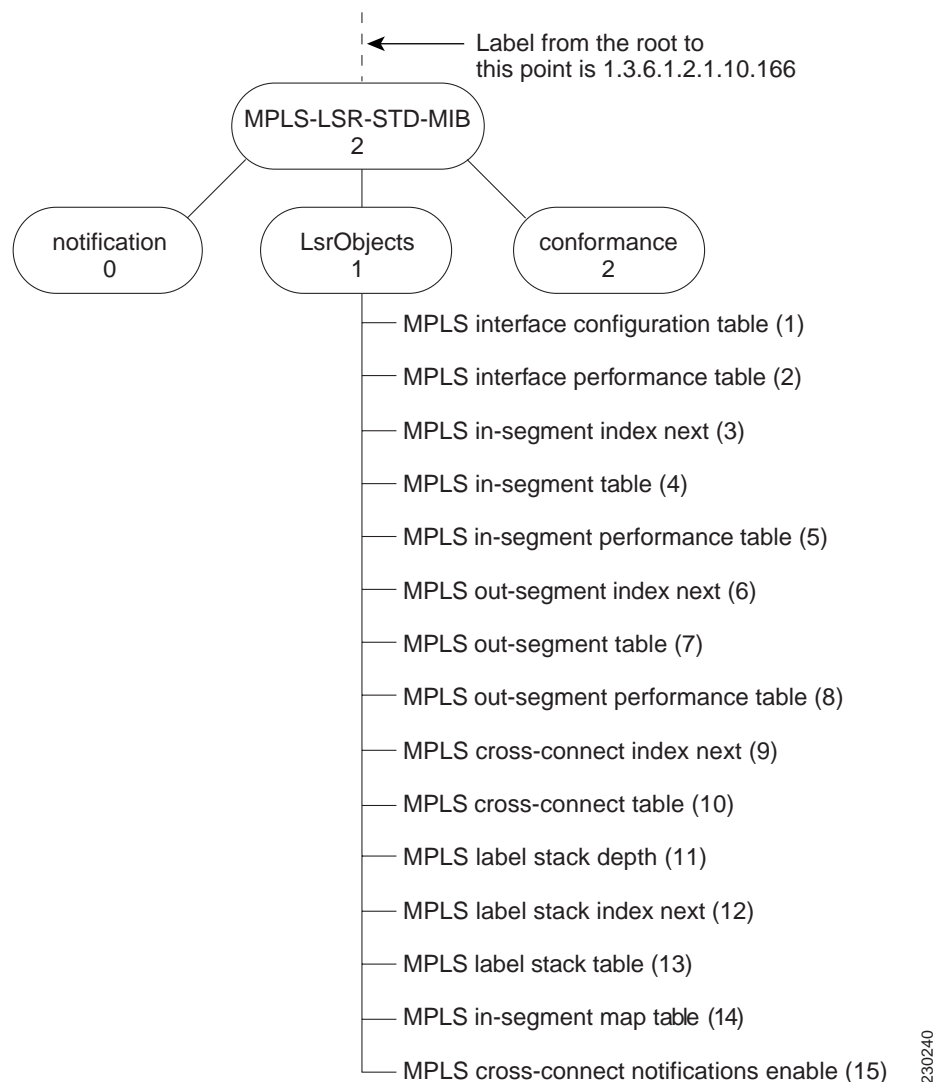
The MPLS-LSR-STD-MIB falls on the branch of the Internet MIB hierarchy represented by the object identifier 1.3.6.1.2.1.10.166. This branch can also be represented by its object name iso.org.dod.internet.mgmt.mib-2.transmission.mplsStdMIB. The MPLS-LSR-STD-MIB is identified by the object name mplsLsrStdMIB, which is denoted by the number 2. Therefore, objects in the MPLS-LSR-MIB can be identified in either of the following ways:

- The object identifier—1.3.6.1.2.1.10.166.2.[MIB-variable]
- The object name—  
iso.org.dod.internet.mgmt.mib-2.transmission.mplsStdMIB.mplsLsrStdMIB.[MIB-variable]

To display a MIB-variable, you enter an SNMP **get** command with an object identifier. Object identifiers are defined by the MPLS-LSR-STD-MIB.

[Figure 5](#) shows the position of the MPLS-LSR-STD-MIB in the Internet MIB hierarchy.



**Figure 5** *MPLS-LSR-STD-MIB in the Internet MIB Hierarchy*

## CLI Commands and the MPLS-LSR-MIB

The MPLS LFIB is the component of the Cisco MPLS subsystem that contains management information for LSRs. You can access this management information by means of either of the following:

- Using the **show mpls forwarding-table** CLI command
- Entering SNMP **get** commands on a network manager

The following examples show how you can gather LSR management information using both methods.

### CLI Command Output

A **show mpls forwarding-table** CLI command allows you to display label forwarding information for a packet on a specific MPLS LSR:

Router# **show mpls forwarding-table**

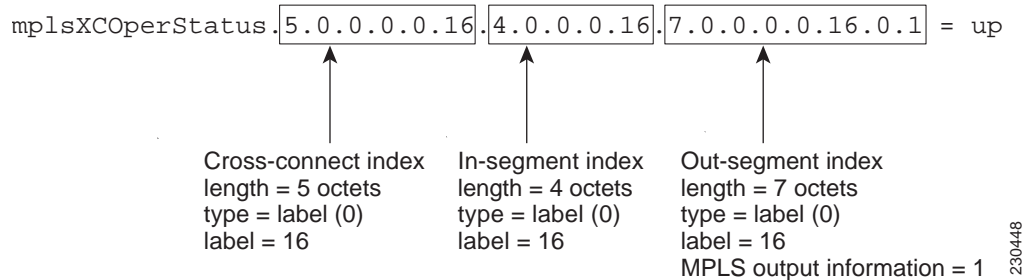
Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
16	Pop Label	IPv4 VRF[V]	1000	aggregate/vpn1	
17	Pop Label	10.0.0.3/32	0	PO7/1/0	point2point
18	Pop Label	10.30.1.0/16	0	PO7/1/0	point2point
19	17	10.0.0.1/32	0	PO7/1/0	point2point
20	No Label	10.9.0.0/16[V]	0	GE3/1	10.30.2.2
21	No Label	10.0.0.7/32[V]	128856	GE3/1	10.30.2.2

### MPLS-LSR-STD-MIB Output

SNMP commands on MIB objects also allow you to display the label forwarding information for a specific MPLS LSR.

You can do a walk-through of the MIB by running a command such as **getmany -v2c public mplsLsrStdMIB** on a network manager where **getmany** does repeated SNMP **getnext** operations to retrieve the contents of the MPLS-LSR-STD-MIB. Figure 6 shows index information for the **mplsXCOperStatus** MPLS-LSR-STD-MIB object and how to read the information in the MIB output that follows.

**Figure 6** Index Information for the **mplsXCOperStatus** MPLS-LSR-STD-MIB Object



```
mplsXCOperStatus.5.0.0.0.0.4.0.0.0.0.7.0.0.0.0.0.1 = up
mplsXCOperStatus.5.0.0.0.0.1.4.0.0.0.1.1.0 = up
mplsXCOperStatus.5.0.0.0.0.2.4.0.0.0.2.7.0.0.0.0.2.0.1 = up
mplsXCOperStatus.5.0.0.0.0.3.4.0.0.0.3.1.0 = up
mplsXCOperStatus.5.0.0.0.0.16.4.0.0.0.16.7.0.0.0.0.16.0.1 = up
mplsXCOperStatus.5.0.0.0.0.17.4.0.0.0.17.7.0.0.0.0.17.0.1 = up
mplsXCOperStatus.5.0.0.0.0.18.4.0.0.0.18.7.0.0.0.0.18.0.1 = up
mplsXCOperStatus.5.0.0.0.0.19.4.0.0.0.19.7.0.0.0.0.19.0.1 = up
mplsXCOperStatus.5.0.0.0.0.20.4.0.0.0.20.1.0 = up
mplsXCOperStatus.5.0.0.0.0.21.4.0.0.0.21.1.0 = up
mplsXCOperStatus.6.2.10.0.0.3.32.1.0.8.2.10.0.0.3.32.0.1 = up
mplsXCOperStatus.6.2.10.30.0.16.1.0.8.2.30.1.0.0.16.0.1 = up
```

You can continue to scan the output of the **getmany** command for the following MIB objects from the MPLS out-segment table:

- Out-segment's top label objects (**mplsOutSegmentTopLabel**)

```
mplsOutSegmentTopLabel.7.0.0.0.0.0.1 = 3
mplsOutSegmentTopLabel.7.0.0.0.0.2.0.1 = 3
```

```

mplsOutSegmentTopLabel.7.0.0.0.0.16.0.1 = 3
mplsOutSegmentTopLabel.7.0.0.0.0.17.0.1 = 3
mplsOutSegmentTopLabel.7.0.0.0.0.18.0.1 = 3
mplsOutSegmentTopLabel.7.0.0.0.0.19.0.1 = 17
mplsOutSegmentTopLabel.8.2.10.0.0.1.32.0.1 = 17
mplsOutSegmentTopLabel.8.2.10.0.0.3.32.0.1 = 3
mplsOutSegmentTopLabel.8.2.10.30.0.16.0.1 = 3

```

- Out-segment's interface (mplsOutSegmentInterface)

```

mplsOutSegmentInterface.7.0.0.0.0.0.0.1 = 0
mplsOutSegmentInterface.7.0.0.0.0.2.0.1 = 0
mplsOutSegmentInterface.7.0.0.0.0.16.0.1 = 0
mplsOutSegmentInterface.7.0.0.0.0.17.0.1 = 55
mplsOutSegmentInterface.7.0.0.0.0.18.0.1 = 55
mplsOutSegmentInterface.7.0.0.0.0.19.0.1 = 55
mplsOutSegmentInterface.8.2.10.0.0.1.32.0.1 = 55
mplsOutSegmentInterface.8.2.10.0.0.3.32.0.1 = 55
mplsOutSegmentInterface.8.2.10.30.0.16.0.1 = 55

```

For more information on how to read the indexing for MPLS-LSR-STD-MIB objects, see [Figure 2](#) and the “[MPLS-LSR-STD-MIB Indexing—Linking Table Elements](#)” section on page 11.

## VPN Aware LSR MIB

Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB include the VPN Aware LSR MIB feature that enables the MPLS-LSR-STD-MIB to get VPN context information. This feature adds support for different contexts for different MPLS VPNs. Users of the MIB can display per-VPN entries in the MPLS-LSR-STD-MIB tables. The VPN Aware LSR MIB feature does not change the syntax of the MPLS-LSR-STD-MIB. It changes the number and types of entries within the tables.

The MPLS-LSR-STD-MIB can show information about only one context at a time. You can specify either a global context or an MPLS VPN context using an SNMP security name. The security name must match the SNMP community name when an SNMP request is performed on a MIB entry.

## SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

VPN-aware SNMP requires that SNMP manager and agent entities operating in a VPN environment agree on mapping between the SNMP security name and the VPN name. This mapping is created by you using different contexts for the SNMP data of different VPNs, which is accomplished through the configuration of the SNMP View-based Access Control Model MIB (SNMP-VACM-MIB). The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space within the context of only that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values within a VPN context:

- The first security phase is authentication of the username. During this phase, the user is authorized for SNMP access.
- The second phase is access control. During this phase, the user is authorized for SNMP access to the group objects in the requested SNMP context.

- In the third phase, the user can access a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VRF instances and SNMP community strings. When a VRF instance is associated with an SNMP community string, SNMP processes requests coming in for a particular community string only if they are received from the configured VRF. If the community string contained in the incoming packet has no VRF associated with it, it is processed only if it came in through a non-VRF interface.

## Major Differences Between the MPLS-LSR-STD-MIB and the MPLS-LSR-MIB

The MPLS-LSR-STD-MIB based on RFC 3813 provides the same basic functionality as the MPLS-LSR-MIB based on Version 05 of the IETF MPLS-LSR-MIB. They both provides an interface for managing label switching through the use of SNMP.

After the implementation of the MPLS-LSR-STD-MIB (RFC 3813) in Cisco IOS Releases 12.2(33)SRB and 12.2(33)SRB, the MPLS-LSR-MIB will exist for a period of time before support is completely removed. This gives you the chance to migrate to the MPLS-LSR-STD-MIB. Both MIBs can coexist in the same image because the MPLS-LSR-STD-MIB and the MPLS-LSR-MIB have different root object identifiers (OIDs).

The following sections contain information about the major differences between the MPLS-LSR-STD-MIB and the MPLS-LSR-MIB:

- [MPLS-LSR-MIB and the MPLS-LSR-STD-MIB Scalar Object Differences, page 17](#)
- [MPLS-LSR-MIB and the MPLS-LSR-STD-MIB Table Object Differences, page 18](#)
- [MPLS-LSR-MIB and MPLS-LSR-STD-MIB Notification Differences, page 22](#)
- [MPLS-LSR-MIB and MPLS-LSR-STD-MIB Indexing Differences, page 22](#)

### MPLS-LSR-MIB and the MPLS-LSR-STD-MIB Scalar Object Differences

Table 10 shows the major difference between the MPLS-LSR-MIB objects and the MPLS-LSR-STD-MIB objects for each scalar object.

**Table 10** *Scalar Objects: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsTrafficParamIndexNext	—	Object deleted.
mplsInSegmentTrapEnable	—	Object deleted.
mplsOutSegmentTrapEnable	—	Object deleted.
—	mplsInSegmentIndexNext	New object.
mplsOutSegmentIndexNext	mplsOutSegmentIndexNext	Syntax change. Formerly integer 32, now is MplsIndexType, which is an octet string.
mplsXCIndexNext	mplsXCIndexNext	Syntax change. Formerly integer 32, now is MplsIndexType, which is an octet string.

## MPLS-LSR-MIB and the MPLS-LSR-STD-MIB Table Object Differences

The following tables show the major differences between the MPLS-LSR-MIB and the MPLS-LSR-STD-MIB for each table.

### MPLS Interface Table (mplsInterfaceTable) Differences

Table 11 shows the difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS interface table (mplsInterfaceTable), formerly called the MPLS interface configuration table (mplsInterfaceConfTable).

**Table 11** *MPLS Interface Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsInterfaceTotalBuffer	—	Object deleted.
mplsInterfaceAvailableBuffer	—	Object deleted.
mplsInterfaceConfStorageType	—	Object deleted.
mplsInterfaceConfIndex	mplsInterfaceIndex	Object name changed.

### MPLS Interface Performance Table (mplsInterfacePerfTable) Differences

Table 12 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS interface performance table (mplsInterfacePerfTable).

**Table 12** *MPLS Interface Performance Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsInterfaceInPackets	—	Object deleted.
mplsInterfaceInDiscards	—	Object deleted.
mplsInterfaceInLabelsUsed	mplsInterfacePerfInLabelsInUse	Object name changed.
mplsInterfaceFailedLabelLookup	mplsInterfacePerfInLabelLookupFailures	Object name changed.
mplsInterfaceOutPackets	—	Object deleted.
mplsInterfaceOutDiscard	—	Object deleted.
mplsInterfaceOutLabelsUsed	mplsInterfacePerfOutLabelsInUse	Object name changed.
mplsInterfaceOutFragments	mplsInterfacePerfOutFragmentedPkts	Object name changed.

### MPLS In-Segment Table (mplsInSegmentTable) Differences

Table 13 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS in-segment table (mplsInSegmentTable).

**Table 13** *MPLS In-Segment Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsInSegmentAdminStatus	—	Object deleted.
mplsInSegmentOperStatus	—	Object deleted.

**Table 13** *MPLS In-Segment Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsInSegmentIfIndex	mplsInSegmentInterface	Object name changed. Formerly not accessible (was used as index into the table). Now it is an object in the table.
—	mplsInSegmentIndex	New object. Used as an index into the table.
—	mplsInSegmentLabelPtr	New object.
mplsInSegmentLabel	mplsInSegmentLabel	Formerly not accessible (was used as index into the table). Now it is an object in the table.
mplsInSegmentXCIndex	mplsInSegmentXCIndex	Syntax change. Formerly Integer32, now MplsIndexType, which is an Octet String.

MPLS In-Segment Performance Table (mplsInSegmentPerfTable) Differences

Table 14 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS in-segment performance table (mplsInSegmentPerfTable).

**Table 14** *MPLS In-Segment Performance Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsInSegmentOctets	mplsInSegmentPerfOctets	Object name changed.
mplsInSegmentPackets	mplsInSegmentPerfPackets	Object name changed.
mplsInSegmentErrors	mplsInSegmentPerfErrors	Object name changed.
mplsInSegmentDiscards	mplsInSegmentPerfDiscards	Object name changed.
mplsInSegmentHCOctets	mplsInSegmentPerfHCOctets	Object name changed.

MPLS Out-Segment Table (mplsOutSegmentTable) Differences

Table 15 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS out-segment table (mplsOutSegmentTable).

**Table 15** *MPLS Out-Segment Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsOutSegmentAdminStatus	—	Object deleted.
mplsOutSegmentOperStatus	—	Object deleted.
mplsOutSegmentIndex	mplsOutSegmentIndex	Syntax changed. Formerly Integer32, now MplsIndexType, which is an octet string.
mplsOutSegmentIfIndex	mplsOutSegmentInterface	Object name changed.

**Table 15** *MPLS Out-Segment Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences (continued)*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
—	mplsOutSgementTopLabelPtr	New object.
mplsOutSegmentNextHopIpAddrType	mplsOutSegmentNextHopAddrType	Object name changed.
mplsOutSegmentNextHopIpv4Addr mplsOutSegmentNextHopIpv6Addr	mplsOutSegmentNextHopAddr	Formerly two objects, now one object with the syntax of InetAddress.
mplsOutSegmentXCIndex	mplsOutSegmentXCIndex	Syntax changed. Formerly Integer32, now MplsIndexType, which is an octet string.

MPLS Out-Segment Performance Table (mplsOutSegmentPerfTable) Differences

Table 16 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS out-segment performance table (mplsOutSegmentPerfTable).

**Table 16** *MPLS Out-Segment Performance Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsOutSegmentOctets	mplsOutSegmentPerfOctets	Object name changed.
mplsOutSegmentPackets	mplsOutSegmentPerfPackets	Object name changed.
mplsOutSegmentErrors	mplsOutSegmentPerfErrors	Object name changed.
mplsOutSegmentDiscards	mplsOutSegmentPerfDiscards	Object name changed.
mplsOutSegmentHCOctets	mplsOutSegmentPerfHCOctets	Object name changed.

MPLS Cross-Connect Table (mplsXCTable) Differences

Table 17 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS cross-connect table (mplsXCTable).

**Table 17** *MPLS Cross-Connect Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsXCIsPersistent	—	Object deleted.
mplsXCIndex	mplsXCIndex	Syntax changed. Formerly Integer32, now MplsIndexType, which is an octet string.
—	mplsXCInSegmentIndex	New object, an index into the mplsXCTable.

**Table 17** *MPLS Cross-Connect Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences (continued)*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
—	mplsXCOutSegmentIndex	New object, an index into the mplsXCTable.
mplsXCLabelStackIndex	mplsXCLabelStackIndex	Syntax changed. Formerly Integer32, now MplsIndexType, which is an octet string.

#### MPLS Label Stack Table (mplsLabelStackTable) Differences

Table 18 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS label stack table (mplsLabelStackTable).

**Table 18** *MPLS Label Stack Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
mplsLabelStackIndex	mplsLabelStackIndex	Syntax changed. Formerly Integer32, now MplsIndexType, which is an octet string.
—	mplsLabelStackLabelPtr	New object.

#### MPLS In-Segment Map Table (mplsInSegmentMapTable) Differences

Table 19 shows the major difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB objects for the MPLS in-segment map table (mplsInSegmentMapTable). The MPLS in-segment map table is a new table introduced with the MPLS-LSR-STD-MIB.

**Table 19** *MPLS In-Segment Map Table: MPLS-LSR-MIB and MPLS-LSR-STD-MIB Object Differences*

MPLS-LSR-MIB Object	MPLS-LSR-STD-MIB Object	Difference
—	mplsInSegmentMapInterface	New object.
—	mplsInSegmentMapLabel	New object.
—	mplsInSegmentMapLabelPtrIndex	New object.
—	mplsInSegmentMapIndex	New object.

#### MPLS Traffic Parameters Table (mplsTrafficParamTable) Differences

The MPLS traffic parameters table was not supported in Cisco IOS implementation of MPLS-LSR-MIB. It has been removed from the MPLS-LSR-STD-MIB.



## MPLS-LSR-MIB and MPLS-LSR-STD-MIB Notification Differences

Table 20 shows the difference between MPLS-LSR-MIB and MPLS-LSR-STD-MIB notifications.

**Table 20** *MPLS-LSR-MIB and MPLS-LSR-STD-MIB Notification Differences*

MPLS-LSR-MIB Notification	MPLS-LSR-STD-MIB Notification	Difference
mplsInSegmentUp	—	Object deleted.
mplsInSegmentDown	—	Object deleted.
mplsOutSegmentUp	—	Object deleted.
mplsOutSegmentDown	—	Object deleted.
mplsXCUp	mplsXCUp	Returned objects changed.
mplsXCDown	mplsXCDown	Returned objects changed.

The following notifications were not supported for MPLS-LSR-MIB and are not supported for the MPLS-LSR-STD-MIB in Cisco IOS Releases 12.2(33)SRB and 12.3(33)SB:

- mplsXCUp
- mplsXCDown



### Note

For scalability reasons, none of the notifications were implemented in the Cisco IOS software from the MPLS-LSR-MIB. For the same reason, the notifications from the MPLS-LSR-STD-MIB are not implemented in Cisco IOS Releases 12.2(33)SRB and 12.2(33)SB.

## MPLS-LSR-MIB and MPLS-LSR-STD-MIB Indexing Differences

One of the major differences between the MPLS-LSR-MIB and the MPLS-LSR-STD-MIB is the indexing used for the three main tables that manage labels for the MPLS LSR in the MPLS-LSR-MIB and the MPLS-LSR-STD-MIB: the MPLS in-segment table (mplsInSegmentTable), the MPLS cross-connect table (mplsXCTable), and the MPLS out-segment table (mplsOutSegmentTable).

All entries in each table are uniquely identified by one or more indexes. The indexes determine the order in which entries are displayed in a MIB walk.

Table 21 compares indexing characteristics of the draft Version 05 MPLS-LSR-MIB implementation with indexing characteristics of the MPLS-LSR-STD-MIB (RFC 3813) implementation.

**Table 21** *Comparison of Indexing Characteristics of the MPLS-LSR-MIB and the MPLS-LSR-STD-MIB*

Object Compared	MPLS-LSR-MIB Draft Version 05 Implementation	MPLS-LSR-STD-MIB RFC 3813 Implementation
Index type definition	A 32-bit integer type is used to define the indexing into the tables that manage label switching in the MPLS LSR.	An octet string is used to define the indexing into the tables that manage label switching in the MPLS LSR.
MPLS in-segment table index	The MPLS in-segment table is indexed by the SNMP interface index (ifIndex) and the incoming label (mplsInSegmentLabel).	The MPLS in-segment table is indexed by the mplsInSegmentIndex. The mplsInSegmentIndex is a 4-byte octet string representing the local label (mplsInSegmentLabel).

**Table 21**      *Comparison of Indexing Characteristics of the MPLS-LSR-MIB and the MPLS-LSR-STD-MIB (continued)*

Object Compared	MPLS-LSR-MIB Draft Version 05 Implementation	MPLS-LSR-STD-MIB RFC 3813 Implementation
MPLS cross-connect table index	The MPLS cross-connect table indexing has four indexes: mplsXCIndex, ifIndex, mplsInSegmentLabel, and mplsOutSegmentIndex. The SNMP interface index and incoming label are identical to the in-segment table. The mplsXCIndex and mplsOutSegmentIndex values are defined as arbitrary unsigned 32-bit quantities.	The MPLS cross-connect table indexing has three indexes: mplsXCIndex, mplsXCInSegmentIndex, and mplsXCOutSegmentIndex. The mplsXCInSegmentIndex is the same as the mplsInSegmentIndex in the in-segment table. The mplsXCOutSegmentIndex is the same as the mplsOutSegmentIndex in the out-segment table.
MPLS out-segment table index	The MPLS out-segment table is indexed by the mplsOutSegmentIndex, which corresponds to the mplsOutSegmentIndex used in the MPLS cross-connect table.	The MPLS out-segment table is indexed by the mplsOutSegmentIndex, which corresponds to the mplsXCIndex with the addition of two bytes that contain an MOI list index.

For more information about the relationship between the indexes for the MPLS-LSR-STD-MIB implementation, see the [“MPLS-LSR-STD-MIB Indexing—Linking Table Elements”](#) section on page 11.

## How to Configure SNMP for the MPLS EM—MPLS LSR MIB - RFC 3813

This section contains tasks to configure the MPLS EM—MPLS LSR MIB (RFC 3813) feature.

The SNMP agent for the MPLS-LSR-STD-MIB is disabled by default and must be enabled for you to use SNMP to monitor and manage the MPLS LSRs on your network. Perform these task to enable the SNMP Agent and verify that it is enabled:

- [Enabling the SNMP Agent, page 24](#) (required)
- [Verifying That the SNMP Agent Is Enabled, page 26](#) (optional)

Perform the following task to configure a VPN context for the MPLS-LSR-STD-MIB:

- [Configuring a VPN-Aware LSR MIB, page 26](#) (optional)

## Prerequisites

The MPLS-LSR-STD-MIB requires the following:

- SNMP installed and enabled on the LSR
- MPLS enabled on the LSR
- MFI

## Enabling the SNMP Agent

To enable the SNMP agent, perform the following task.

The SNMP agent for the MPLS-LSR-STD-MIB is disabled by default.

### SUMMARY STEPS

1. **enable**
2. `show running-config`
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6 nacl**] [*access-list-number*]
5. **end**
6. `save running-config startup-config`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
	<b>Example:</b> <code>Router&gt; enable</code>	
Step 2	<code>show running-config</code>	Displays the running configuration of the router to determine if an SNMP agent is already running on the device.
	<b>Example:</b> <code>Router# show running-config</code>	If no SNMP information is displayed, continue with the next step.  If any SNMP information is displayed, you can modify the information or change it as desired.
Step 3	<code>configure terminal</code>	Enters global configuration mode.
	<b>Example:</b> <code>Router# configure terminal</code>	

	Command or Action	Purpose
Step 4	<pre>snmp-server community string [view view-name] [ro   rw] [ipv6 nacl] [access-list-number]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server community public ro</pre>	<p>Sets up the community access string to permit access to SNMP.</p> <ul style="list-style-type: none"> <li>The <i>string</i> argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string.</li> <li>The <b>view</b> <i>view-name</i> keyword-argument pair is the name of a previously defined view. The view defines the objects available to the SNMP community.</li> <li>The <b>ro</b> keyword specifies read-only access. Authorized management stations can retrieve only MIB objects.</li> <li>The <b>rw</b> keyword specifies read-write access. Authorized management stations can retrieve and modify MIB objects.</li> <li>The <b>ipv6 nacl</b> keywords specify the IPv6 named access list.</li> <li>The <i>access-list-number</i> argument is an integer from 1 to 99. It specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent.</li> </ul> <p>Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers. Devices at these addresses are allowed to use the community string to gain access to the SNMP agent.</p>
Step 5	<pre>end</pre> <p><b>Example:</b></p> <pre>Router(config)# end</pre>	Exits to privileged EXEC mode.
Step 6	<pre>save running-config startup-config</pre> <p><b>Example:</b></p> <pre>Router# save running-config startup-config</pre>	Saves the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.

## Verifying That the SNMP Agent Is Enabled

To verify that the SNMP agent is enabled, perform the following task.

### SUMMARY STEPS

1. **telnet** *device-ip-address*
2. **enable**
3. **show running-config**
4. **exit**

### DETAILED STEPS

---

**Step 1** **telnet** *device-ip-address*

Use this command to access the router through a Telnet session. For example:

```
Prompt> telnet 10.15.230.20
```

where 10.15.20.20 represents the IP address of the target device.

**Step 2** **enable**

Use this command to enable privileged EXEC mode. Enter your password, if prompted. For example:

```
Router> enable
Router#
```

**Step 3** **show running-config**

Use this command to display the running configuration. Look for SNMP information. For example:

```
Router# show running-config
.
.
.
snmp-server community public RO
```

If you see any “snmp-server” statements, SNMP has been enabled on the router.

**Step 4** **exit**

Use this command to exit privileged EXEC mode. For example:

```
Router# exit
Router>
```

---

## Configuring a VPN-Aware LSR MIB

To configure a VPN-aware LSR MIB, perform the following tasks:

- [Configuring SNMP Support for a VPN, page 27](#) (required)
- [Configuring an SNMP Context for a VPN, page 28](#) (required)
- [Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2, page 30](#) (required)

## Configuring SNMP Support for a VPN

To configure SNMP support for a VPN (or a remote VPN), perform the following task. SNMP support for VPNs allows users of the MPLS-LSR-STD-MIB to display per-VPN entries in the MPLS-LSR-STD-MIB tables.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server engineID remote** {*ipv4-address* | *ipv6-address*} [**udp-port** *udp-port-number*] [**vrf** *vrf-name*] *engineid-string*
4. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server engineID remote</b> { <i>ipv4-address</i>   <i>ipv6-address</i> } [ <b>udp-port</b> <i>udp-port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ] <i>engineid-string</i>  <b>Example:</b> Router(config)# snmp-server engineID remote 172.16.20.3 vrf customer1 80000009030000B064EFE100	Specifies the SNMP engine ID of a remote SNMP device. <ul style="list-style-type: none"> <li>• The <i>ipv4-address</i> argument is the IPv4 address of the device that contains the remote copy of SNMP.</li> <li>• The <i>ipv6-address</i> argument is the IPv6 address of the device that contains the remote copy of SNMP.</li> <li>• The <b>udp-port</b> keyword specifies a User Datagram Protocol (UDP) port of the host to use.</li> <li>• The <i>udp-port-number</i> argument is the socket number on the remote device that contains the remote copy of SNMP. The default is 161.</li> <li>• The <b>vrf</b> keyword specifies an instance of a routing table.</li> <li>• The <i>vrf-name</i> argument is the name of the VRF table to use for storing data.</li> <li>• The <i>engineid-string</i> is a string of a maximum of 24 characters that identifies the engine ID.</li> </ul>
Step 4	<b>end</b>  <b>Example:</b> Router(config)# end	Exits to privileged EXEC mode.

## What to Do Next

Proceed to the [““Configuring an SNMP Context for a VPN” section on page 28.](#)

## Configuring an SNMP Context for a VPN

To configure an SNMP context for a VPN, perform the following task. This sets up a unique SNMP context for a VPN that allows you to access the per-VPN entries in the VRF table.

### SNMP Context

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about users of other VPNs on the same networking device.

### VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables for a VPN. Cisco IOS software adds the RD to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

Either the RD is an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter an RD in either of these formats:

- 16-bit ASN: your 32-bit number, for example, 101:3.
- 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server context** *context-name*
4. **ip vrf** *vrf-name*
5. **rd** *route-distinguisher*
6. **context** *context-name*
7. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>snmp-server context context-name</b>  <b>Example:</b> Router(config)# snmp-server context context-vpn1	Creates an SNMP context. <ul style="list-style-type: none"> <li>The <i>context-name</i> argument is the name of the SNMP context being created.</li> </ul>
Step 4	<b>ip vrf vrf-name</b>  <b>Example:</b> Router(config)# ip vrf customer1	Configures a VRF table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument is the name assigned to a VRF.</li> </ul>
Step 5	<b>rd route-distinguisher</b>  <b>Example:</b> Router(config-vrf)# rd 100:1	Creates routing and forwarding tables for a VRF. <ul style="list-style-type: none"> <li>The <i>route-distinguisher</i> argument specifies to add an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.</li> </ul>
Step 6	<b>context context-name</b>  <b>Example:</b> Router(config-vrf)# context context-vpn1	Associates an SNMP context with a particular VRF. <ul style="list-style-type: none"> <li>The <i>context-name</i> argument is the name of the SNMP VPN context, up to 32 characters.</li> </ul>
Step 7	<b>route-target {import   export   both}</b> <b>route-target-ext-community</b>  <b>Example:</b> Router(config-vrf)# route-target export 100:1	(Optional) Creates a route-target extended community for a VRF. <ul style="list-style-type: none"> <li>The <b>import</b> keyword specifies to import routing information from the target VPN extended community.</li> <li>The <b>export</b> keyword specifies to export routing information to the target VPN extended community.</li> <li>The <b>both</b> keyword specifies to import both import and export routing information to the target VPN extended community.</li> <li>The <i>route-target-ext-community</i> argument adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.</li> </ul>
Step 8	<b>end</b>  <b>Example:</b> Router(config-vrf)# end	Exits to privileged EXEC mode.



## What to Do Next

Proceed to the [“Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2”](#) section on page 30.

## Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2

To configure a VPN-aware SNMP context for SNMPv1 or SNMPv2, perform the following task. This allows you to access per-VPN entries in the MPLS-LSR-STD-MIB tables using SNMPv1 or SNMPv2.

### SNMPv1 or SNMPv2 Security

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP Versions 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP Version 3 performs.

To configure the VPN Aware LSR MIB feature when using SNMP Version 1 or SNMP Version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if they come in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, the packet is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from using a clear text community string to query the VPN data. However, this is not as secure as using SNMPv3.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote host** [**udp-port port**]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access access-list**]
4. **snmp-server group** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context context-name**] [**read readview**] [**write writeview**] [**notify notifyview**] [**access access-list**]
5. **snmp-server view** *view-name oid-tree* {**included** | **excluded**}
6. **snmp mib community-map** *community-name* [**context context-name**] [**engineid engine-id**] [**security-name security-name**] **target-list** *vpn-list-name*
7. **snmp mib target list** *vpn-list-name* {**vrf vrf-name** | **host ip-address**}
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>snmp-server user username group-name [remote host [udp-port port]] {v1   v2c   v3 [encrypted] [auth {md5   sha} auth-password]} [access access-list]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server user vrfcomm-vpn1 group-vpn1 v2c</pre>	<p>Configures a new user to an SNMP group.</p> <ul style="list-style-type: none"> <li>• The <i>username</i> argument is the name of the user on the host that connects to the agent.</li> <li>• The <i>group-name</i> argument is the name of the group to which the user belongs.</li> <li>• The <b>remote</b> <i>host</i> keyword and argument specify a remote SNMP entity to which the user belongs, and the hostname or IPv6 address or IPv4 IP address of that entity. If both an IPv6 address and IPv4 IP address are being specified, the IPv6 host must be listed first.</li> <li>• The <b>udp-port</b> <i>port</i> keyword and argument specify the UDP port number of the remote host. The default is UDP port 162.</li> <li>• The <b>vi</b> keyword specifies that SNMPv1 should be used.</li> <li>• The <b>v2c</b> keyword specifies that SNMPv2c should be used.</li> <li>• The <b>v3</b> keyword specifies that the SNMPv3 security model should be used. Allows the use of the <b>encrypted</b> and or <b>auth</b> keywords.</li> <li>• The <b>encrypted</b> keyword specifies whether the password appears in encrypted format (a series of digits, masking the true characters of the string).</li> <li>• The <b>auth</b> keyword specifies which authentication level should be used.</li> <li>• The <b>md5</b> keyword is the HMAC-MD5-96 authentication level.</li> <li>• The <b>sha</b> keyword is the HMAC-SHA-96 authentication level.</li> <li>• The <i>auth-password</i> argument is a string (not to exceed 64 characters) that enables the agent to receive packets from the host. The minimum length for a password is one character. The recommended length of a password is at least eight characters, and should include both letters and numbers.</li> <li>• The <b>access</b> <i>access-list</i> keyword and argument specify an access list to be associated with this SNMP user.</li> </ul>

	Command or Action	Purpose
<p><b>Step 4</b></p>	<pre>snmp-server group group-name {v1   v2c   v3 {auth   noauth   priv}} [context context-name] [read readview] [write writeview] [notify notifyview] [access access-list]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server group group-vpn1 v2c context context-vpn1 read view-vpn1 write view-vpn1 notify *tv.00000000.00040000.00000000.0 access context-vpn1</pre>	<p>Configures a new SNMP group or a table that maps SNMP users to SNMP views.</p> <ul style="list-style-type: none"> <li>• The <i>group-name</i> argument is the name of the group.</li> <li>• The <b>vi</b> keyword specifies that SNMPv1 should be used for the group.</li> <li>• The <b>v2c</b> keyword specifies that SNMPv2c should be used for the group. The SNMPv2c security model allows for the transmission of informs, and supports 64-character strings (instead of 32-character strings).</li> <li>• The <b>v3</b> keyword specifies that the SNMPv3 should be used for the group. SMNPv3 is the most secure of the supported security models, because it allows you to explicitly configure the authentication characteristics.</li> <li>• The <b>auth</b> keyword specifies authentication of a packet without encrypting it.</li> <li>• The <b>noauth</b> keyword specifies no authentication of a packet.</li> <li>• The <b>priv</b> keyword specifies authentication of a packet with encryption.</li> <li>• The <b>context</b> <i>context-name</i> keyword and argument associate the specified SNMP group with a configured SNMP context.</li> <li>• The <b>read</b> <i>readview</i> keyword and argument specify a read view for the SNMP group. The <i>readview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to display only the contents of the agent.</li> <li>• The <b>write</b> <i>writeview</i> keyword and argument specify a write view for the SNMP group. The <i>writeview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to enter data and configure the contents of the agent.</li> <li>• The <b>notify</b> <i>notifyview</i> keyword and argument specify a notify view for the SNMP group. The <i>writeview</i> argument represents a string (not to exceed 64 characters) that is the name of the view that enables you to specify a notify, inform, or trap.</li> <li>• The <b>access</b> <i>access-list</i> keyword and argument specify a standard access list (a standard ACL) to associate with the group.</li> </ul>

	Command or Action	Purpose
Step 5	<p><b>snmp-server view</b> <i>view-name oid-tree</i> {<b>included</b>   <b>excluded</b>}</p> <p><b>Example:</b> Router(config)# snmp-server view view-vpn1 iso included</p>	<p>Creates or updates a view entry.</p> <ul style="list-style-type: none"> <li>The <i>view-name</i> argument is the label for the view record that you are updating or creating. The name is used to reference the record.</li> <li>The <i>oid-tree</i> argument is the object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Replace a single subidentifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.</li> <li>The <b>included</b> keyword configures the OID (and subtree OIDs) specified in the <i>oid-tree</i> argument to be included in the SNMP view.</li> <li>The <b>excluded</b> keyword configures the OID (and subtree OIDs) specified in the <i>oid-tree</i> argument to be explicitly excluded from the SNMP view.</li> </ul>
Step 6	<p><b>snmp mib community-map</b> <i>community-name</i> [<b>context</b> <i>context-name</i>] [<b>engineid</b> <i>engine-id</i>] [<b>security-name</b> <i>security-name</i>] <b>target-list</b> <i>vpn-list-name</i></p> <p><b>Example:</b> Router(config)# snmp mib community-map vrfcomm-vpn1 context context-vpn1 target-list targ-vpn1</p>	<p>Associates an SNMP community with an SNMP context, Engine ID, or security name.</p> <ul style="list-style-type: none"> <li>The <i>community-name</i> argument is an SNMP community string.</li> <li>The <b>context</b> <i>context-name</i> keyword and argument specify an SNMP context name to be mapped to the SNMP community.</li> <li>The <b>engineid</b> <i>engine-id</i> keyword and argument specify an SNMP engine ID to be mapped to the SNMP community.</li> <li>The <b>security-name</b> <i>security-name</i> keyword and argument specify the security name to be mapped to the SNMP community.</li> <li>The <b>target-list</b> <i>vpn-list-name</i> keyword and argument specify the VRF list to be mapped to the SNMP community. The list name should correspond to a list name used in the <b>snmp mib target list</b> command.</li> </ul>

	Command or Action	Purpose
Step 7	<pre>snmp mib target list vpn-list-name {vrf vrf-name   host ip-address}</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp mib target list targ-vpn1 vrf customer1</pre>	<p>Creates a list of target VRFs and hosts to associate with an SNMP community.</p> <ul style="list-style-type: none"> <li>• The <i>vpn-list-name</i> argument is the name of the target list.</li> <li>• The <b>vrf</b> keyword adds a specified VRF to the target list.</li> <li>• The <i>vrf-name</i> argument is the name of a VRF to include in the list.</li> <li>• The <b>host</b> keyword adds a specified host to the target list.</li> <li>• The <i>ip-address</i> argument is the IP address of the host.</li> </ul>
Step 8	<pre>end</pre> <p><b>Example:</b></p> <pre>Router(config) end</pre>	<p>Exits to privileged EXEC mode.</p>

## Configuration Examples for the MPLS EM—MPLS LSR MIB - RFC 3813

This section contains the following configuration examples for the MPLS EM—MPLS LSR MIB - RFC 3813 feature:

- [Enabling the SNMP Agent: Examples, page 35](#)
- [Configuring a VPN-Aware LSR MIB: Example, page 36](#)

### Enabling the SNMP Agent: Examples

The following example shows how to enable an SNMP agent.

```
Router# configure terminal
Router(config)# snmp-server community
```

In the following example, SNMPv1 and SNMPv2C are enabled. The configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

In the following example, read-only access is allowed for all objects to members of access list 4 that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro 4
```

## Configuring a VPN-Aware LSR MIB: Example

This section contains the following examples for configuring a VPN-aware LSR MIB:

- [Configuring SNMP Support for a VPN: Example, page 36](#)
- [Configuring an SNMP Context for a VPN: Example, page 36](#)
- [Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2: Example, page 36](#)

### Configuring SNMP Support for a VPN: Example

The following example shows how to configure SNMP support for a VPN:

```
configure terminal
!
snmp-server engineID remote 172.16.20.3 vrf vrf customer1 80000009030000B064EFE100
end
```

### Configuring an SNMP Context for a VPN: Example

The following example shows how to configure an SNMP context for a VPN. In this example, the VPN vrf1 is associated with the SNMP context context1.

```
configure terminal
!
snmp-server context context-vpn1
ip vrf customer1
rd 100:1
context context-vpn1
route-target export 100:1
end
```

### Configuring a VPN-Aware SNMP Context for SNMPv1 or SNMPv2: Example

The following configuration example shows how to configure a VPN-aware SNMP context for the MPLS LSR MIB with SNMPv1 or SNMPv2:

```
snmp-server context context-vpn1

ip vrf customer1
rd 100:1
context context-vpn1
route-target export 100:1
route-target import 100:1
!
!
interface Ethernet1/0
ip vrf forwarding customer1
ip address 10.99.99.100 255.0.0.0
mpls label protocol ldp
mpls ip
!
!
interface Serial3/0
ip vrf forwarding customer1
ip address 10.60.1.1 255.0.0.0
mpls label protocol ldp
mpls ip
serial restart-delay 0
```

```

!
ip access-list standard context-vpn1

!
snmp-server group group-vpn1 v2c context context-vpn1 read view-vpn1 notify
*tv.00000000.00040000.00000000.0 access context-vpn1
!
snmp-server view view-vpn1 iso included
!
snmp-server community public RW
snmp-server community vrfcomm-vpn1 RW1
!
snmp-server user vrfcomm-vpn1 vrfcomm-vpn1 v1
snmp-server user vrfcomm-vpn1 group-vpn1 v2c
!

snmp mib community-map vrfcomm-vpn1 context context-vpn1 target-list targ-vpn1
!
snmp mib target list targ-vpn1 host 0.0.0.0
snmp mib target list targ-vpn1 vrf customer1
!

```

## Additional References

The following sections provide references related to the MPLS EM—MPLS LSR MIB - RFC 3813 feature.

## Related Documents

Related Topic	Document Title
Configuring SNMP using Cisco IOS software	<a href="#">“Configuring SNMP Support” chapter in the <i>Cisco IOS Network Management Configuration Guide</i></a>
SNMP command descriptions	<a href="#">Cisco IOS Network Management Command Reference</a>
SNMP support for VPNs	<a href="#">SNMP Notification Support for VPNs</a>
SNMP context support for VPNs configuration tasks	<a href="#">SNMP Support over VPNs—Context Based Access Control</a>
MPLS concepts and configuration tasks	<a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—



## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>MPLS-LSR-MIB</li> <li>MPLS-LSR-STD-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 3291	<i>Textual Conventions for Internet Network Addresses</i>
RFC 3413	<i>Simple Network Management Protocol (SNMP) Applications</i>
RFC 3812	<i>Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)</i>
RFC 3813	<i>Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

This feature uses no new or modified commands.

# Feature Information for MPLS EM—MPLS LSR MIB - RFC 3813

Table 22 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 22 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

**Table 22** Feature Information for MPLS EM—MPLS LSR MIB - RFC 3813

Feature Name	Releases	Feature Information
MPLS EM—MPLS LSR MIB - RFC 3813	12.2(33)SRB 12.2(33)SB	<p>The MPLS LSR MIB- RFC 3813 (MPLS-LSR-STD-MIB) allows you to use the Simple Network Management Protocol (SNMP) to remotely monitor a label switch router (LSR) that is using the Multiprotocol Label Switching (MPLS) technology.</p> <p>This document describes the MPLS-LSR-STD-MIB. The document also describes the major differences between the MPLS-LSR-STD-MIB and draft Version 5 of the MPLS-LSR-MIB.</p> <p>The MPLS EM—MPLS LSR MIB - RFC 3813 feature introduces the MPLS-LSR-STD-MIB, which is an upgrade from draft Version 5 of the MPLS-LSR-MIB to an implementation of the <i>Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)</i>, RFC 3813. This feature also introduces the VPN Aware LSR MIB feature that enables the MPLS-LSR-STD-MIB to get VPN context information.</p> <p>Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks in line with the fault, configuration, accounting, performance, and security (FCAPS) model.</p> <p>In 12.2(33)SRB, this feature was introduced.</p> <p>In 12.2(33)SB, this feature was integrated into a Cisco IOS 12.2SB release.</p>

**Table 22**      **Feature Information for MPLS EM—MPLS LSR MIB - RFC 3813 (continued)**

Feature Name	Releases	Feature Information
		<p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS-LSR-STD-MIB Benefits</a>, page 3</li> <li>• <a href="#">Label Switching Information Managed by the MPLS-LSR-STD-MIB</a>, page 4</li> <li>• </li> <li>• <a href="#">MPLS-LSR-STD-MIB Elements</a>, page 5</li> <li>• <a href="#">Brief Description of MPLS-LSR-STD-MIB Tables</a>, page 5</li> <li>• <a href="#">MPLS LSR Information Available Through the MPLS-LSR-STD-MIB</a>, page 5</li> <li>• <a href="#">Information from MPLS-LSR-STD-MIB Scalar Objects</a>, page 10</li> <li>• <a href="#">MPLS-LSR-STD-MIB Indexing—Linking Table Elements</a>, page 11</li> <li>• <a href="#">Interface Configuration Table and Interface MIB Links</a>, page 12</li> <li>• <a href="#">MPLS-LSR-STD-MIB Structure</a>, page 13</li> <li>• <a href="#">Major Differences Between the MPLS-LSR-STD-MIB and the MPLS-LSR-MIB</a>, page 17</li> <li>• <a href="#">Enabling the SNMP Agent</a>, page 24</li> <li>• <a href="#">Verifying That the SNMP Agent Is Enabled</a>, page 26</li> </ul> <p>No commands were introduced or modified for this feature.</p>

# Glossary

**cross-connect (XC)**—An association of in-segments and incoming MPLS interfaces to out-segments and outgoing MPLS interfaces.

**FPI**—forwarding path identifier. An identifier required to locate MPLS forwarding information for a FEC. Examples of types of FPIs supported by the MPLS Forwarding Infrastructure (MFI) are IPv4, IPv6, LABEL, SSS, and TE.

**IETF**—Internet Engineering Task Force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

**inSegment**—A label on an incoming packet that is used to determine the forwarding of the packet.

**label**—A short, fixed-length identifier that is used to determine the forwarding of a packet.

**label switching**—A term used to describe the forwarding of IP (or other network layer) packets using a label swapping algorithm based on network layer routing algorithms. The forwarding of these packets uses the exact match algorithm and rewrites the label.

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

**LFIB**—Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

**LSP**—label switched path. A sequence of hops in which a packet travels from one router to another router by means of label switching mechanisms. A label-switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

**LSR**—label switching router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MFI**—MPLS Forwarding Infrastructure. In the Cisco MPLS subsystem, the data structure for storing information about incoming and outgoing labels and associated equivalent packets suitable for labeling.

**MIB**—Management Information Base. Database of network management information that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved by means of SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MOI**—MPLS output information. The MOI includes the next hop, outgoing interface, and outgoing label.

**MPLS**—Multiprotocol Label Switching. MPLS is a method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**MPLS interface**—An interface on which MPLS traffic is enabled.

**NMS**—Network Management Station. A device (usually a workstation) that performs SNMP queries to the SNMP agent of a managed device in order to retrieve or modify information.

**notification request**—Message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. SNMP notification requests are more reliable than traps, because a notification request from an SNMP agent requires that the SNMP manager acknowledge receipt of the notification request. The manager replies with an SNMP response protocol data unit (PDU). If the manager does not receive a notification message from an SNMP agent, it does not send a response. If the sender (SNMP agent) never receives a response, the notification request can be sent again. Thus, a notification request is more likely than a trap to reach its intended destination.

**outSegment**—A label on an outgoing packet.

**SNMP**—Simple Network Management Protocol. Management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**trap**—Message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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

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



# MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

---

**First Published: January 7, 2008**

**Last Updated: April 11, 2008**

The MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature document describes the MPLS-L3VPN-STD-MIB that supports Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Networks (VPNs) based on RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*, and describes the major differences between RFC 4382 and MPLS-VPN-MIB, which is based on the Internet Engineering Task Force (IETF) draft Version 3 (draft-ietf-ppvpn-mpls-vpn-mib-03.txt). This document also describes the changes needed to implement MPLS-L3VPN-STD-MIB (RFC 4382). The MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB provide an interface for managing the MPLS VPN feature in Cisco IOS software through the use of the Simple Network Management Protocol (SNMP).

Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks according to the fault, configuration, accounting, performance, and security (FCAPS) model.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade” section on page 43](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 2](#)
- [Restrictions for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 2](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Information About MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 2](#)
- [How to Configure MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 30](#)
- [Configuration Examples for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 38](#)
- [Additional References, page 40](#)
- [Command Reference, page 42](#)
- [Feature Information for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade, page 43](#)
- [Glossary, page 45](#)

## Prerequisites for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

The MPLS-L3VPN-STD-MIB agent requires the following:

- SNMP is installed and enabled on the label switching routers (LSRs).
- MPLS is enabled on the LSRs.
- Multiprotocol Border Gateway Protocol (BGP) is enabled on the LSRs.
- Cisco Express Forwarding is enabled on the LSRs.
- Label Distribution Protocol (LDP) paths or traffic-engineered tunnels (RFC 3812) are configured between provider edge (PE) routers and customer edge (CE) routers.

## Restrictions for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

The following is not supported for Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB:

- Configuration of the MIB using the SNMP SET command is not supported, except for the trap-related object, `mplsL3VpnNotificationEnable`.

## Information About MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

This section contains the following topics:

- [MPLS Layer 3 VPN Overview, page 3](#)
- [MPLS-L3VPN-STD-MIB Benefits, page 3](#)
- [Capabilities Supported by the MPLS-L3VPN-STD-MIB, page 3](#)
- [Supported Objects in the MPLS-L3VPN-STD-MIB, page 4](#)
- [MPLS-L3VPN-STD-MIB Scalar Objects, page 5](#)
- [MPLS-L3VPN-STD-MIB MIB Tables, page 6](#)
- [MPLS-L3VPN-STD-MIB Notification Events, page 18](#)
- [MPLS-L3VPN-STD-MIB Support for IPv6 VPNs over MPLS, page 21](#)
- [MPLS-L3VPN-STD-MIB Data Security, page 24](#)
- [Major Differences Between the MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB, page 25](#)

## MPLS Layer 3 VPN Overview

The MPLS Layer 3 VPN technology allows service providers to offer intranet and extranet VPN services that directly connect their customers' remote offices to a public network with the same security and service levels that a private network offers. Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF is created for each VPN defined on a router and contains most of the information needed to manage and monitor MPLS Layer 3 VPNs: an IP routing table, a derived Cisco Express Forwarding table, a set of interfaces that use this forwarding table, and a set of rules and routing protocol parameters that control the information that is included in the routing table.

## MPLS-L3VPN-STD-MIB Benefits

The MPLS-L3VPN-STD-MIB provides access to VRF information, and to interfaces included in the VRF, and other configuration and monitoring information.

The MPLS-L3VPN-STD-MIB provides the following benefits:

- A standards-based SNMP interface for retrieving information about critical MPLS VPN events.
- VRF information to assist in the management and monitoring of MPLS VPNs.
- Information, in conjunction with the Interfaces MIB, about interfaces assigned to VRFs.
- Performance statistics for all VRFs on a router.
- The generation and queueing of notifications that call attention to major changes in the operational status of MPLS VPN enabled interfaces and the forwarding of notification messages to a designated network management system (NMS) for evaluation and action by network administrators.
- Warning when VPN routing tables are approaching or exceed their capacity.
- Warnings about the reception of illegal labels on a VRF-enabled interface. Such receptions may indicate misconfiguration or an attempt to violate security.

## Capabilities Supported by the MPLS-L3VPN-STD-MIB

SNMP agent code operating with the MPLS-L3VPN-STD-MIB enables a standardized, SNMP-based approach to managing MPLS VPNs in Cisco IOS software.

The MPLS-L3VPN-STD-MIB is based on RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base*, which includes objects describing features that support MPLS VPN events.

The MPLS-L3VPN-STD-MIB provides you with the ability to do the following:

- Gather routing and forwarding information for MPLS VPNs on a router.
- Display information in the VRF routing table.
- Send notification messages that signal changes when critical MPLS VPN events occur.
- Enable, disable, and configure notification messages for MPLS VPN events by using extensions to existing SNMP command-line interface (CLI) commands.
- Specify the IP address of an NMS in the operating environment to which notification messages are sent.
- Write notification configurations into nonvolatile memory.



Some slight differences between RFC 4382 and the actual implementation of MPLS VPNs within Cisco IOS software require some minor translations between the MPLS-L3VPN-STD-MIB and the internal data structures of Cisco IOS software. These translations are accomplished by means of the SNMP agent code. Also, while running as a low priority process, the SNMP agent provides a management interface to Cisco IOS software. SNMP adds minimal overhead on the normal functions of the device.

All MPLS-L3VPN-STD-MIB objects are based on RFC 4382; thus, no Cisco-specific SNMP application is required to support the functions and operations pertaining to the MPLS-L3VPN-STD-MIB features.

## Supported Objects in the MPLS-L3VPN-STD-MIB

The MPLS-L3VPN-STD-MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS VPN feature in Cisco IOS software. The MPLS-L3VPN-STD-MIB conforms to Abstract Syntax Notation One (ASN.1), thus providing an idealized MPLS VPN database.

Using any standard SNMP network management application, you can retrieve and display information from the MPLS-L3VPN-STD-MIB using GET operations; similarly, you can traverse information in the MIB database for display using GETNEXT operations.

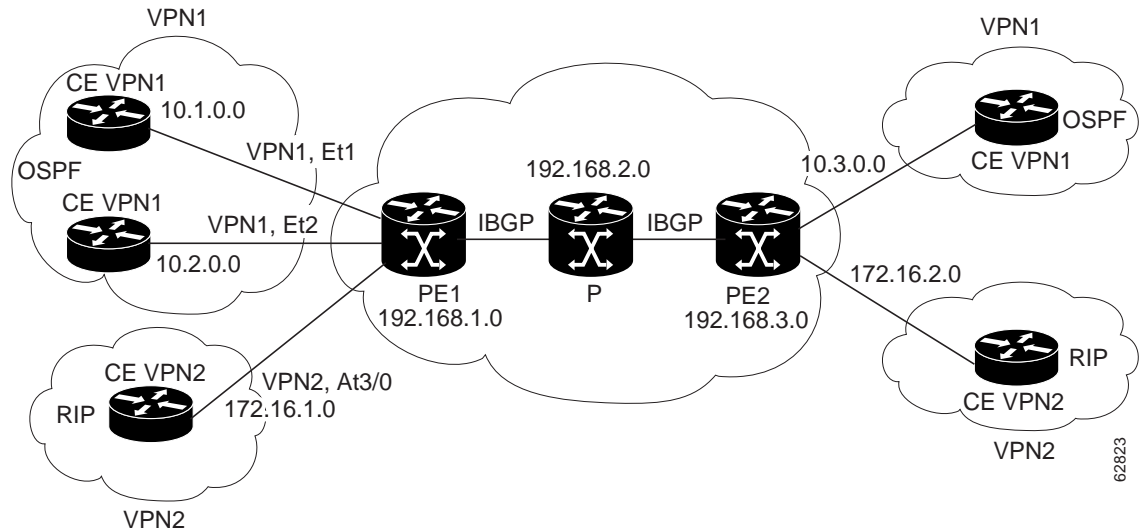
The MPLS-L3VPN-STD-MIB tables and objects are described briefly in the following sections:

- [MPLS-L3VPN-STD-MIB Scalar Objects, page 5](#)
- [MPLS-L3VPN-STD-MIB MIB Tables, page 6](#)
- [MPLS-L3VPN-STD-MIB Notification Events, page 18](#)

[Figure 1](#) shows a simple MPLS VPN configuration. This configuration includes two customer MPLS VPNs (labeled VPN1 and VPN2) and a simple provider network that consists of two PE routers (labeled PE1 and PE2) and a provider core router labeled P. [Figure 1](#) shows the following sample configuration:

- VRF names—VPN1 and VPN2
- Interfaces associated with VRFs—Et1, Et2, and At3/0
- Routing protocols—Open Shortest Path First (OSPF), Routing Information Protocol (RIP), and Interior Border Gateway Protocol (IBGP)
- Routes associated with VPN1—10.1.0.0, 10.2.0.0, and 10.3.0.0
- Routes associated with VPN2—172.16.1.0 and 172.16.2.0
- Routes associated with the provider network—192.168.1.0, 192.168.2.0, and 192.168.3.0

This configuration is used to explain MPLS VPN events that are monitored and managed by the MPLS-L3VPN-STD-MIB.

**Figure 1**      **Sample MPLS Layer 3 VPN Configuration**

For information on IPv6 VPN over MPLS (6VPE) configuration, see the “Implementing IPv6 VPN over MPLS (6VPE)” chapter in the *Cisco IOS IPv6 Configuration Guide*.

## MPLS-L3VPN-STD-MIB Scalar Objects

MPLS-L3VPN-STD-MIB defines several scalar objects. [Table 1](#) describes the scalar objects that are implemented for Cisco IOS Release 12.2(33)SRC and Release 12.2(33)SB.

**Table 1**      **MPLS-L3VPN-STD-MIB Scalar Objects**

MIB Object	Description
mplsL3VpnConfiguredVrfs	The number of VRFs configured on the router, including VRFs recently deleted.
mplsL3VpnActiveVrfs	The number of VRFs that are active on the router. An active VRF is assigned to at least one interface that is in the operationally up state.
mplsL3VpnConnectedInterfaces	The total number of interfaces assigned to a VRF.
mplsL3VpnNotificationEnable	<p>An object to enable or disable MPLS-L3VPN-STD-MIB notifications:</p> <ul style="list-style-type: none"> <li>Setting this object to true enables all notifications defined in the MPLS-L3VPN-STD-MIB.</li> <li>Setting this object to false disables all notifications defined in the MIB. This is the default.</li> </ul> <p>This is one of the few objects that is writable.</p>
mplsL3VpnVrfConfMaxPossRts	The number of routes that this router is capable of storing. This value cannot be determined because it is based on the amount of available memory in the system. Therefore, this object is set to zero (0).

**Table 1** *MPLS-L3VPN-STD-MIB Scalar Objects (continued)*

MIB Object	Description
mplsL3VpnVrfConfRteMxThrshTime	<p>An interval in seconds in which repeat mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notifications can be sent if there is an attempt to continuously add routes after the maximum route limit is reached.</p> <p>The default value is 0. When the value is 0, the MIB agent does not send the notification again unless the number of routes drops below the threshold and attempts to exceed the threshold again.</p> <p>You can set the number of seconds after which the maximum threshold notification is sent with the following configuration command:</p> <pre>Router(config)# snmp mib mpls vpn max-threshold seconds</pre>
mplsL3VpnIlIlLblRcvThrsh	<p>A number above which the receipt of an illegal label generates an mplsNumVrfSecIlIlglLblThrshExcd notification. The default value is 0.</p> <p>You can set the number of illegal labels that generate a notification with the following configuration command:</p> <pre>Router(config)# snmp mib mpls vpn illegal-label number</pre>

## MPLS-L3VPN-STD-MIB MIB Tables

The MPLS-L3VPN-STD-MIB implementation supports the tables described in the following sections:

- [VRF Configuration Table \(mplsL3VpnVrfTable\), page 6](#)
- [VPN Interface Configuration Table \(mplsL3VpnIfConfTable\), page 10](#)
- [VRF Route Target Table \(mplsL3VpnVrfRTTable\), page 11](#)
- [VRF Security Table \(mplsL3VpnVrfSecTable\), page 13](#)
- [VRF Performance Table \(mplsL3VpnVrfPerfTable\), page 13](#)
- [VRF Routing Table \(mplsL3VpnVrfRteTable\), page 14](#)

### VRF Configuration Table (mplsL3VpnVrfTable)

Entries in the VRF configuration table (mplsL3VpnVrfTable) represent the VRF instances that are configured on the router. These include recently deleted VRFs. The information in this table is also displayed in the output of the **show vrf detail** command.

Each VRF is referenced by its VRF name (mplsL3VpnVrfName).

[Table 2](#) lists MPLS Layer 3 VPN information and the associated MIB objects supported by the VRF configuration table (mplsL3VpnVrfTable).

**Table 2**      **VRF Configuration Table—MPLS Layer 3 VPN Information and Associated MIB Objects**

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnVrfName	<p>The name associated with this VRF. When this object is used as an index to a table, the first octet is the string length, and subsequent octets are the ASCII codes of each character. For example, “vpn1” is represented as 4.118.112.110.49.</p> <p>The VRF name can be equivalent to the VPN ID. If the VRF name is equivalent to the VPN ID, the VRF name must be equivalent to the value for the mplsL3VpnVrfVpnId MIB object. We recommend that all sites that support VRFs that are part of the same VPN use the same naming convention for VRFs and use the same VPN ID.</p>
mplsL3VpnVrfVpnId	The VPN identification number based on RFC 2685. If you do not specify a VPN ID, the value is an empty string.
mplsL3VpnVrfDescription	<p>The description of the VRF. This is specified with the <b>description</b> command in VRF configuration mode:</p> <pre>Router(config)# vrf definition vrf-name Router(config-vrf)# description vrf-description</pre> <p><b>Note</b> You can use the <b>vrf definition vrf-name</b> command to configure both IPv6 and IPv4 address-family VRFs. When you use the <b>ip vrf vrf-name</b> command, you can configure only an IPv4 address-family VRF.</p>
mplsL3VpnVrfRD	<p>The route distinguisher for this VRF. This is specified with the <b>rd</b> command in VRF configuration mode:</p> <pre>Router(config)# vrf definition vrf-name Router(config-vrf)# rd route-distinguisher</pre> <p><b>Note</b> You can use the <b>vrf definition vrf-name</b> command to configure both IPv6 and IPv4 address-family VRFs. When you use the <b>ip vrf vrf-name</b> command, you can configure only an IPv4 address-family VRF.</p>
mplsL3VpnVrfCreationTime	The value of the sysUpTime when this VRF entry was created.
mplsL3VpnVrfOperStatus	<p>The operational status of this VRF. A VRF is up (1) when at least one interface associated with the VRF is up. A VRF is down (2) when:</p> <ul style="list-style-type: none"> <li>• No interfaces exist whose ifOperStatus = up (1).</li> <li>• No interfaces are associated with this VRF.</li> </ul>
mplsL3VpnVrfActiveInterfaces	The number of interfaces assigned to this VRF that are operationally up.
mplsL3VpnVrfAssociatedInterfaces	The number of interfaces assigned to this VRF, independent of the operational status.

**Table 2**      **VRF Configuration Table—MPLS Layer 3 VPN Information and Associated MIB Objects (continued)**

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnVrfConfMidRteThresh	<p>The middle threshold. If the number of routes in the VRF crosses this threshold, an mplsL3VpnVrfRouteMidThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in VRF address family configuration mode as a percentage of the maximum with the <b>maximum routes limit {warn-threshold   warn-only}</b> command.</p> <p>For example, the following <b>maximum routes</b> command sets the warning threshold for an IPv4 address family in VRF vpn1 as 50 percent of the maximum route threshold:</p> <pre>Router(config)# vrf definition vpn1 Router(config-vrf)# address-family ipv4 Router(config-vrf-af)# maximum routes 1000 50</pre> <p>If vpn1 also has an IPv6 address family configured, the following <b>maximum routes</b> command sets the warning threshold for the IPv6 address family as 50 percent of its maximum route threshold:</p> <pre>Router(config)# vrf definition vpn1 Router(config-vrf)# address-family ipv6 Router(config-vrf-af)# maximum routes 2000 50</pre> <p><b>Note</b>    The <b>vrf definition vrf-name</b> command can configure both IPv6 and IPv4 address-family VRFs. When you use the <b>ip vrf vrf-name</b> command, you can configure only an IPv4 address-family VRF.</p> <p>If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the warning threshold values. In this example, the aggregate warning threshold is 1500 routes [(ipv4 = 500) + (ipv6 = 1000)]. An mplsL3VpnVrfRouteMidThreshExceeded notification is not sent until both address families reach their warning threshold. If only a single address family exists for the VRF, the mplsL3VpnVrfRouteMidThreshExceeded notification is sent when the warning threshold is reached for the single address family.</p> <p>The following command sets a middle threshold of 1000 routes. An mplsL3VrfRouteMidThreshExceeded notification is sent when this threshold is exceeded. However, additional routes are still allowed because a maximum route threshold is not set with this command.</p> <pre>Router(config-vrf-if)# maximum routes 1000 warn-only</pre> <p>See the “<a href="#">MPLS-L3VPN-STD-MIB Notification Events</a>” section on page 18 for more information on the mplsL3VpnVrfRouteMidThreshExceeded notification.</p>

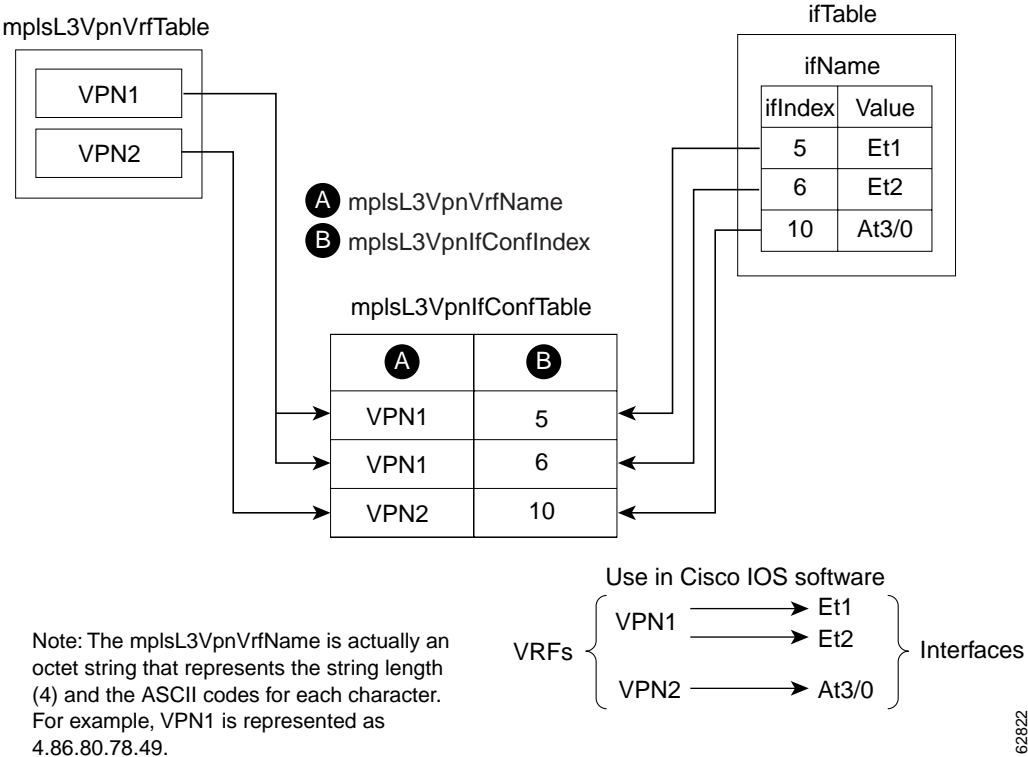
**Table 2** VRF Configuration Table—MPLS Layer 3 VPN Information and Associated MIB Objects (continued)

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnVrfConfHighRteThresh	<p>The maximum route threshold. If the number of routes in the VRF crosses this threshold, an mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is sent (if notifications are enabled and configured). You can set this value in VRF address family configuration mode with the <b>maximum routes limit</b> {<i>warn-threshold</i>   <b>warn-only</b>} command as follows:</p> <pre>Router(config)# vrf definition vpn2 Router(config-vrf)# address-family ipv4 Router(config-vrf-af)# maximum routes 1000 75  Router(config)# vrf definition vpn2 Router(config-vrf)# address-family ipv6 Router(config-vrf-af)# maximum routes 2000 75</pre> <p><b>Note</b> The <b>vrf definition vrf-name</b> command can configure both IPv6 and IPv4 address-family VRFs. When you use the <b>ip vrf vrf-name</b> command, you can configure only an IPv4 address-family VRF.</p> <p>If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the maximum threshold values. In this example, the aggregate maximum route threshold is 3000 [(ipv4 = 1000)+ (ipv6 = 2000)]. An mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification is not sent until both address families reaches their maximum route threshold. If only a single address family exists for the VRF, the mplsL3VpnVrfRouteMaxThreshExceeded notification is sent when the maximum route threshold is reached for the single address family. Routes are not added to the address-family that has already reached its maximum route threshold.</p> <p>See the “<a href="#">MPLS-L3VPN-STD-MIB Notification Events</a>” section on page 18 for more information on the mplsL3VpnVrfNumVrfRouteMaxThreshExceeded notification.</p>
mplsL3VpnVrfConfMaxRoutes	This value is the same as that for mplsL3VpnVrfConfHighRteThresh.
mplsL3VpnVrfConfLastChanged	<p>The value of sysUpTime when the configuration of the VRF changes or interfaces are assigned or unassigned from the VRF.</p> <p><b>Note</b> This object is updated only when values in this table change.</p>
mplsL3VpnVrfConfRowStatus	The status of a row in the table. This object normally reads “active (1),” but may read “notInService (2)” if a VRF was recently deleted.
mplsL3VpnVrfConfAdminStatus	<p>The operation status of the VRF. The possible values are:</p> <ul style="list-style-type: none"> <li>up (1)—At least one interface is administratively up and the VRF is ready to pass packets.</li> <li>down (2)—All interfaces are administratively down and the VRF cannot pass packets.</li> </ul>
mplsL3VpnVrfConfStorageType	The storage type for the VRF entry. This object always returns a value of “volatile (2).”

VPN Interface Configuration Table (mplsL3VpnIfConfTable)

In Cisco IOS software, a VRF is associated with one MPLS Layer 3 VPN. Zero or more interfaces can be associated with a VRF. A VRF uses an interface that is defined in the ifTable of the Interfaces Group of MIB II (IFMIB). The IFMIB defines objects for managing interfaces. The ifTable of this MIB contains information on each interface in the network. The mplsL3VpnIfConfTable associates a VRF from the mplsL3VpnVrfTable with a forwarding interface from the ifTable. Figure 2 shows the relationship between VRFs and interfaces defined in the ifTable and the mplsL3VpnIfConfTable.

Figure 2 VRFs, the Interfaces MIB, and the mplsL3VpnIfConfTable



Entries in the VPN interface configuration table (mplsL3VpnIfConfTable) represent the interfaces that are assigned to each VRF. The information available in this table is also displayed in the output of the **show vrf** command.

The mplsL3VpnIfConfTable shows how interfaces are assigned to VRFs. An LSR creates an entry in this table for every interface capable of supporting MPLS Layer 3 VPNs.

The mplsL3VpnIfConfTable is indexed by the following:

- mplsL3VpnVrfName—The VRF name
- mplsL3VpnIfConfIndex—An identifier that is the same as the ifIndex from the Interface MIB of the interface assigned to the VRF

Table 3 lists MPLS Layer 3 VPN information and the associated MIB objects supported by the VPN interface configuration table (mplsL3VpnIfConfTable).

62822

**Table 3**      **VPN Interface Configuration Table—MPLS Layer 3 VPN Information and Associated MIB Objects**

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnIfConfIndex	Provides the interface MIB ifIndex of this interface that is assigned to a VRF.
mplsL3VpnIfVpnClassification	Specifies what type of VPN this interface is providing: carrier supporting carrier (CsC) (1), enterprise (2), or InterProvider (3).  This value is set to enterprise (2) if MPLS is not enabled and to carrier supporting carrier (1) if MPLS is enabled on this interface.
mplsL3VpnIfVpnRouteDistProtocol	Indicates the route distribution protocols that are being used to redistribute routes across the PE-to-CE link on this interface: none (0), BGP (1), OSPF (2), RIP (3), Intermediate System-Intermediate System (IS-IS) (4), static (5), or other (6). More than one protocol can be enabled at the same time.  In Cisco IOS software, router processes are defined and redistributed on a per-VRF basis, not per-interface. Therefore, all interfaces assigned to the same VRF have the same value for this object.
mplsL3VpnIfConfStorageType	Indicates the storage type for the VPN interface entry. The default value for this object is “volatile (2).”
mplsL3VpnIfConfRowStatus	Provides the status of the row in the table that associates the specified interface with the VRF. This object normally reads “active (1),” but may read “notInService (2),” if a VRF was recently deleted.

## VRF Route Target Table (mplsL3VpnVrfRTTable)

The VRF route target table (mplsL3VpnVrfRTTable) describes the route target communities that are defined for a particular VRF. An LSR creates an entry in this table for each target configured for a VRF supporting an MPLS Layer 3 VPN instance.

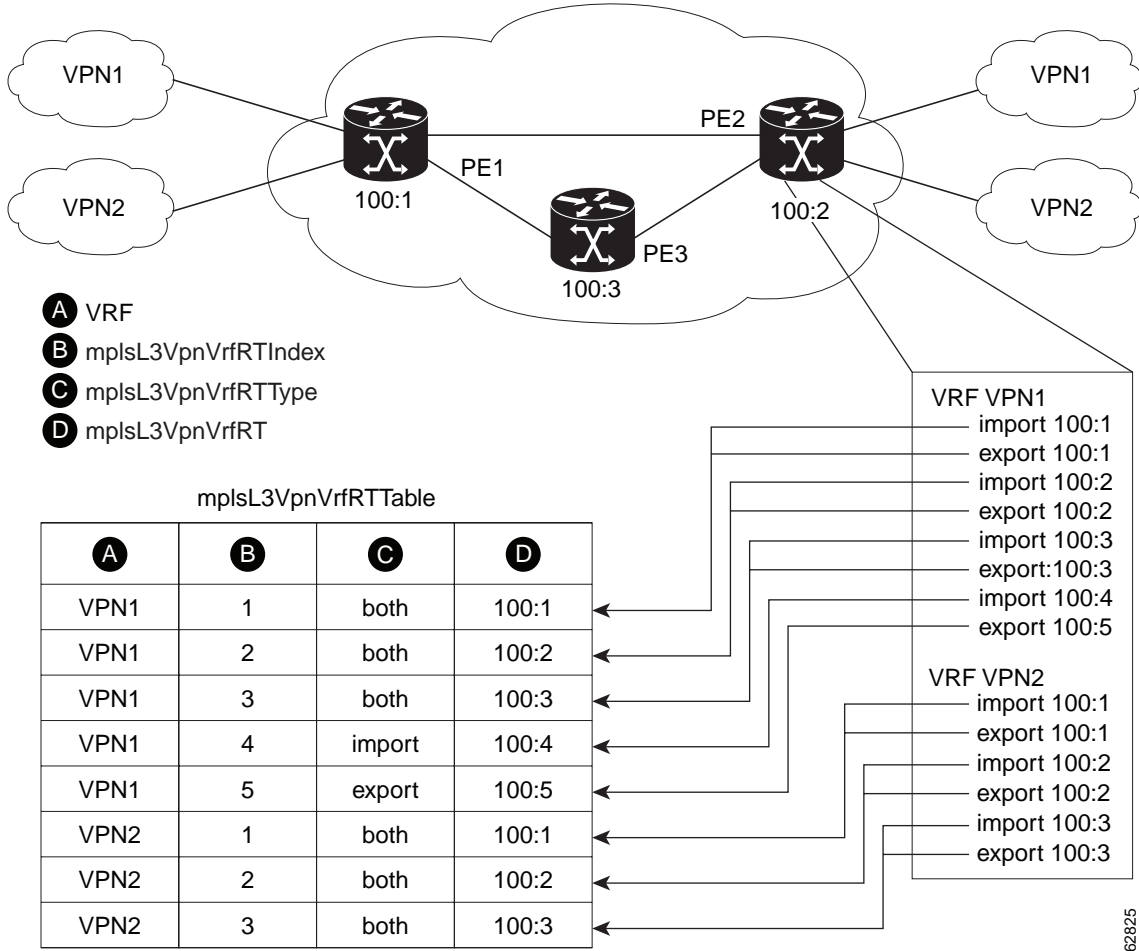
The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. Distribution of VPN routing information works as follows:

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

Figure 3 shows a sample configuration and its relationship to an mplsL3VpnVrfRTTable. A route target table exists on each PE router. Routers with route distinguishers (RDs) 100:1, 100:2, and 100:3 are shown in the sample configuration. Routers with RDs 100:4 and 100:5 are not shown in Figure 3, but are included in the route targets for PE2 and in the mplsL3VpnVrfRTTable.



Figure 3 Sample Configuration and the mplsL3VpnVrfRTTable



Note: The mplsL3VpnVrfName is actually an octet string that represents the string length (4) and the ASCII codes for each character. For example, VPN1 is represented as 4.86.80.78.49.

The mplsL3VpnVrfRTTable shows the import and export route targets for each VRF. The table is indexed by the following:

- mplsL3VpnVrfName—The VRF name
- mplsL3VpnVrfRTIndex—The route target entry identifier
- mplsL3VpnVrfRTType—A value specifying whether the entry is an import route target, is an export route target, or is defined as both

Table 4 lists MPLS Layer 3 VPN information and the associated MIB objects supported by the VRF route target table (mplsL3VpnVrfRTTable).

62825

**Table 4** VRF Route Target Table—MPLS Layer 3 VPN Information and Associated MIB Objects

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnVrfRTIndex	A value that defines each route target's position in the table.
mplsL3VpnVrfRTType	The route target distribution type: import (1), export (2), or both (3).
mplsL3VpnVrfRT	The route target distribution policy. Determines the route distinguisher for this target.
mplsL3VpnVrfRTDescr	This object contains a string that indicates the address family in which the route target was declared. If the route target was declared in an IPv4 address family, the value of this object is AF_IPv4. If the route target was declared in an IPv6 address family, the value of this object is AF_IPv6.
mplsL3VpnVrfRTRowStatus	The status of the row in the table. This object normally reads "active (1)," but may read "notInService (2)" if a VRF was recently deleted.
mplsL3VpnVrfRTStorageType	The storage type for the VPN route target entry. The default value for this object is "volatile (2)."

## VRF Security Table (mplsL3VpnVrfSecTable)

The VRF security table (mplsL3VpnVrfSecTable) provides information about security for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS Layer 3 VPNs.

The mplsL3VpnVrfSecTable augments the mplsL3VpnVrfTable and has the same indexing.

[Table 5](#) lists MPLS Layer 3 VPN information and the associated MIB objects supported by the VRF security table (mplsL3VpnVrfSecTable).

**Table 5** VRF Security Table—MPLS Layer 3 VPN Information and Associated MIB Objects

MIB Object	MPLS Layer 3 Information
mplsL3VpnVrfSecIllegalLblVltns	<p>The number of illegally received labels on a VRF interface. Only illegal labels are counted by this object, therefore the object applies only to a VRF interface that is MPLS-enabled (carrier supporting carrier [CsC] situation).</p> <p>This counter is incremented whenever a label is received that is above or below the valid label range, is not in the global label forwarding table, or is received on the wrong VRF (that is, table IDs for the receiving interface and appropriate VRF label forwarding table do not match).</p> <p><b>Note</b> Discontinuities can occur at reinitialization of the management system and at other times are indicated by the value of the mplsL3VpnVrfSecDiscontinuityTime object.</p>
mplsL3VpnVrfSecDiscontinuityTime	The value of sysUpTime when any one or more of this entry's counters last had a discontinuity. A switchover would cause a discontinuity. If no discontinuities occurred since the last reinitialization of the local management system, this object contains a value of 0.

## VRF Performance Table (mplsL3VpnVrfPerfTable)

The VRF performance table (mplsL3VpnVrfPerfTable) provides statistical performance information for each VRF. An LSR creates an entry in this table for every VRF capable of supporting MPLS Layer 3 VPNs.

The mplsL3VpnVrfPerfTable augments the mplsL3VpnVrfTable and has the same indexing.

Table 6 lists the MPLS Layer 3 VPN information and the associated MIB objects supported by the VRF performance table (mplsL3VpnVrfPerfTable).

**Table 6 VRF Performance Table—MPLS Layer 3 VPN Information and Associated MIB Objects**

MIB Object	MPLS Layer 3 VPN Information
mplsL3VpnVrfPerfRoutesAdded	<p>The value of this counter is the number of routes added to this VRF since the last discontinuity. Discontinuities can occur at reinitialization of the management system (such as on a switchover) and at other times are indicated by the value of the mplsL3VpnVrfPerfDiscTime object.</p> <p>If both IPv4 and IPv6 address-family configurations are present in the VRF, the value of this counter is the sum of the number of routes from the IPv4 and IPv6 routing tables that are added to the VRF.</p>
mplsL3VpnVrfPerfRoutesDeleted	<p>The value of this counter is the number of routes removed from this VRF.</p> <p><b>Note</b> Discontinuities can occur at reinitialization of the management system and at other times are indicated by the value of the mplsL3VpnVrfPerfDiscTime object.</p> <p>If both IPv4 and IPv6 address-family configurations are present in the VRF, the value of this counter is the sum of the number of routes from the IPv4 and IPv6 routing tables that have been deleted from the VRF.</p>
mplsL3VpnVrfPerfCurrNumRoutes	<p>The number of routes currently defined within this VRF.</p> <p>If both IPv4 and IPv6 address-family configurations are present in the VRF, the number of routes is the sum of the number of routes defined for the IPv4 and IPv6 address families in the VRF.</p>
mplsL3VpnVrfPerfRoutesDropped	This object is not supported. The counter always returns a value of 0.
mplsL3VpnVrfPerfDiscTime	The value of sysUpTime when any one or more of this entry's counters had a discontinuity. A switchover would cause a discontinuity. If no discontinuities occurred since the last reinitialization of the local management subsystem, this object contains a value of 0.

## VRF Routing Table (mplsL3VpnVrfRteTable)

The VRF routing table (mplsL3VpnVrfRteTable) provides per-interface routing table information for each MPLS Layer 3 VPN VRF.

The information available in this table can also be displayed with the **show ip route vrf vrf-name** command for IPv4 routes or the **show ipv6 route vrf vrf-name** command for IPv6 routes.

- For example, for PE1 in Figure 1, with the **show ip route vrf vpn1** command, you would see results like the following:

```
Router# show ip route vrf vpn1
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```

* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
      10.0.0.0/32 is subnetted, 3 subnets
B       10.3.0.0 [200/0] via 192.168.2.1, 04:36:33
C       10.1.0.0/16 is directly connected, Ethernet1
C       10.2.0.0/16 [200/0] directly connected Ethernet2, 04:36:33

```

- With the **show ip route vrf vpn2** command, you would see results like the following:

```

Router# show ip route vrf vpn2

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
!
Gateway of last resort is not set
!
      172.16.0.0/32 is subnetted, 2 subnets
B       172.16.2.0 [200/0] via 192.168.2.1, 04:36:33
C       172.16.1.0 is directly connected, ATM 3/0

```

- The following is sample IPv6 output associated with a VRF named vrf3 that you would see with the **show ipv6 route vrf** command:

```

Router# show ipv6 route vrf vrf3

IPv6 Routing Table vrf3 - 6 entries

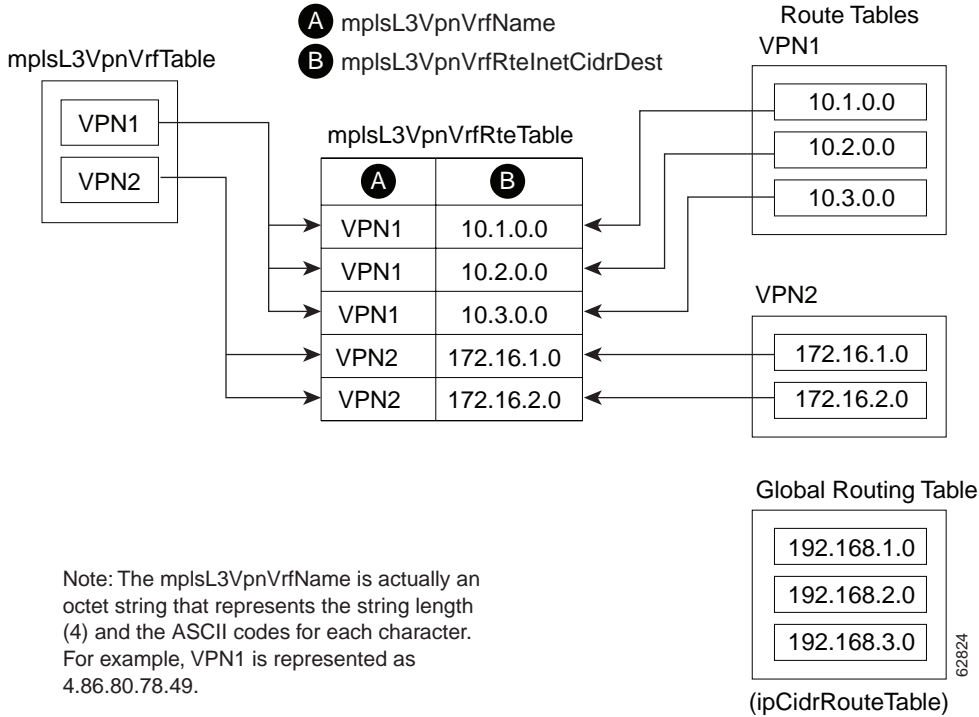
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

C    2001:8::/64 [0/0]
     via ::, FastEthernet0/0
L    2001:8::3/128 [0/0]
     via ::, FastEthernet0/0
B    2002:8::/64 [200/0]
     via ::FFFF:192.168.1.4,
B    2010::/64 [20/1]
     via 2001:8::1,
C    2012::/64 [0/0]
     via ::, Loopback1
L    2012::1/128 [0/0]
     via ::, Loopback1

```

Figure 4 shows the relationship of the routing tables, the VRFs, and the `mplsL3VpnVrfRteTable`. You can display information about the VPN1 and VPN2 route tables using the **show ip route vrf vrf-name** command. The global route table for IPv4 routes is the same as `ipCidrRouteTable` in the IP-FORWARD-MIB. You can display information about the global route table with the **show ip route** command.

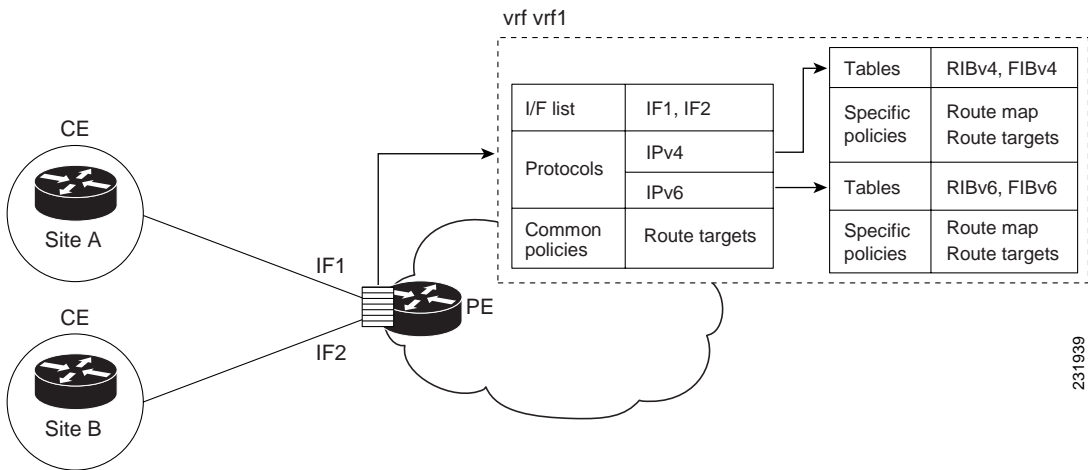
Figure 4 IPv4 Route Table, VRFs, and the mplsL3VpnVrfRteTable



You can display information about IPv6 route tables using the **show ipv6 route vrf {vrf-name | vrf-number}** command. The global route table for IPv6 routes is the same as inetCidrRouteTable in the IP-FORWARD-MIB. You can display information about the global route table with the **show ipv6 route** command.

Figure 5 illustrates a multiprotocol VRF, in which the VRF named vrf1 is enabled for both IPv4 and IPv6 routes and is associated with two interfaces (IF1, IF2), two sets of tables (IPv4 RIB and FIB and IPv6 RIB and FIB), and a set of common or distinct policies.

Figure 5 Multiprotocol VRF



231939

An LSR creates an entry in the `mplsL3VpnVrfRteTable` for every route that is configured, either dynamically or statically, within the context of a specific VRF capable of supporting MPLS Layer 3 VPNs.

The `mplsL3VpnVrfRteTable` is indexed by the following:

- `mplsL3VpnVrfName`—The VRF name, which provides the VRF routing context
- `mplsL3VpnVrfRteInetCidrDestType`—The destination address type (IPv4 or IPv6)
- `mplsL3VpnVrfRteInetCidrDest`—The destination IPv4 or IPv6 address
- `mplsL3VpnVrfRteInetCidrPfxLen`—The length of the prefix for the IP destination address
- `mplsL3VpnVrfRteInetCidrPolicy`—An index that distinguishes between multiple paths to the same destination
- `mplsL3VpnVrfRteInetCidrNHopType`—The address type of the next hop IP address (IPv4 or IPv6)
- `mplsL3VpnVrfRteInetCidrNextHop`—The IP address of the next hop for each route entry

[Table 7](#) lists MPLS Layer 3 VPN information for the MIB objects supported by the VRF routing table (`mplsL3VpnVrfRteTable`). This table represents VRF-specific routes. The global routing table is the `ipCidrRouteTable` (IPv4 routes) or `inetCidrRouteTable` (IPv6 routes) in the IP-FORWARD-MIB.

**Table 7 VRF Routing Table—MPLS Layer 3 VPN Information and Associated MIB Objects**

MIB Object	MPLS LAYER 3 VPN Information
<code>mplsL3VpnVrfRteInetCidrDestType</code>	The address type of the IP destination address. This object has a value of <code>ipv4</code> (1) or <code>ipv6</code> (2).
<code>mplsL3VpnVrfRteInetCidrDest</code>	The destination IP address defined for this route. The type of this address is determined by the value of the <code>mplsL3VpnVrfRteInetCidrDestType</code> object.  The values for the index objects <code>mplsL3VpnVrfRteInetCidrDest</code> and <code>mplsL3VpnVrfRteInetCidrPfxLen</code> must be consistent.
<code>mplsL3VpnVrfRteInetCidrPfxLen</code>	The length of the prefix for the destination address ( <code>mplsL3VpnVrfRteInetCidrDest</code> ).  The values for the index objects <code>mplsL3VpnVrfRteInetCidrDest</code> and <code>mplsL3VpnVrfRteInetCidrPfxLen</code> must be consistent.
<code>mplsL3VpnVrfRteInetCidrPolicy</code>	An index used to distinguish between multiple paths to the same destination. The default value is (0 0).
<code>mplsL3VpnVrfRteInetCidrNHopType</code>	The address type of the next hop IP address. This object has the following values: <code>unknown</code> (0), <code>ipv4</code> (1), <code>ipv6</code> (2), or <code>ipv6z</code> (4). The value should be set to <code>unknown</code> (0) for routes that are not remote.
<code>mplsL3VpnVrfRteInetCidrNextHop</code>	The next hop IP address defined for this route. The type of this address is determined by the <code>mplsL3VpnVrfRteInetCidrNHopType</code> object.
<code>mplsL3VpnVrfRteInetCidrIfIndex</code>	The interface MIB <code>ifIndex</code> for the interface through which this route is forwarded. The object is 0 if no interface is defined for the route.
<code>mplsL3VpnVrfRteInetCidrType</code>	The type of route. The value <code>local</code> (3) indicates a route for which the next hop is the final destination. The value <code>remote</code> (4) is for a route for which the next hop is not the final destination.
<code>mplsL3VpnVrfRteInetCidrProto</code>	The routing protocol that was responsible for adding this route to the VRF.
<code>mplsL3VpnVrfRteInetCidrAge</code>	The number of seconds since this route was last updated.

**Table 7** *VRF Routing Table—MPLS Layer 3 VPN Information and Associated MIB Objects (continued)*

MIB Object	MPLS LAYER 3 VPN Information
mplsL3VpnVrfRteInetCidrNextHopAS	The autonomous system number of the next hop for this route. This object is not supported and is always 0.
mplsL3VpnVrfRteInetCidrMetric1	The primary routing metric used for this route.
mplsL3VpnVrfRteInetCidrMetric2 mplsL3VpnVrfRteInetCidrMetric3 mplsL3VpnVrfRteInetCidrMetric4 mplsL3VpnVrfRteInetCidrMetric5	Alternate routing metrics used for this route. These objects are supported only for Cisco Interior Gateway Routing Protocol (IGRP) and Cisco Enhanced Interior Gateway Routing Protocol (EIGRP) protocols. These objects display the bandwidth metrics used for the route. Otherwise, these values are set to –1.
mplsL3VpnVrfRteXCPointet	This object is not supported. It returns an empty string.  The cross-connect index for the entry associated with the VRF route table entry is in the MPLS Cross-Connect table (mplsXCTable) in the MPLS-LSR-STD-MIB.
mplsL3VpnVrfRteInetCidrStatus	Status of the row. This object normally reads active (1), but may read notInService (2) if a VRF was recently deleted. A row entry cannot be modified when the row status is active (1).

## MPLS-L3VPN-STD-MIB Notification Events

The following notifications of the MPLS-L3VPN-STD-MIB are supported:

- **mplsL3VpnVrfUp**—This notification indicates that the VRF is up. It is generated and sent to an NMS when one interface associated with the VRF is brought up, after previously all interfaces were in the down state.
- **mplsL3VpnVrfDown**—This notification indicates that the VRF is down. It is generated and sent to the NMS when the last interface associated with the VRF is brought down, after all other interfaces associated with the VRF are already in the down state.
- **mplsL3VpnVrfRouteMidThreshExceeded**—This notification is generated and sent when the middle or warning threshold, **mplsL3VpnVrfMidRouteThreshold**, is crossed. You can configure this threshold in the CLI by using the following commands:

```
Router(config)# vrf definition vrf-name
Router(config-vrf)# address-family {ipv4 | ipv6}
Router(config-vrf-af)# maximum routes limit warn-threshold [% of max]
```

The *warn-threshold* argument is a percentage of the maximum routes specified by the *limit* argument. You can also configure a middle threshold with the following command, in which the *limit* argument represents the warning threshold:

```
Router(config-vrf-af)# maximum routes limit warn-only
```

This notification is sent to the NMS only at the time the threshold is exceeded. (See [Figure 6](#) for a comparison of the warning and maximum thresholds.) Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.

If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the warning threshold values. An **mplsL3VpnVrfRouteMidThreshExceeded** notification is not sent until the second address family reaches its warning threshold.

- **mplsL3VpnVrfNumVrfRouteMaxThreshExceeded**—This notification is generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes indicated by the **mplsL3VpnVrfMaxRouteThreshold** object. The maximum number of routes is defined by the *limit* argument of the **maximum routes** commands:

```
Router(config)# vrf definition vrf-name
Router(config-vrf)# address-family {ipv4 | ipv6}
Router(config-vrf-af)# maximum routes limit warn-threshold [% of max]
```

A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another **mplsL3VpnVrfNumVrfRouteMaxThreshExceeded** notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again or if the time interval is reached when the **mplsL3VpnVrfConfRteMxThreshTime** value is nonzero. (See [Figure 6](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.)

If an attempt is made to add routes beyond the route limit, SNMP sends a single notification. No other notification is sent until the route count drops below the route limit and another attempt is made to add routes beyond the limit.

However, if you configure the **snmp mib mpls vpn max-threshold time** command with a value other than 0 (0 is the default), SNMP repeats sending of the notification after the time interval passes if an attempt is made to add another route.

If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the maximum threshold values. An **mplsL3VpnVrfNumVrfRouteMaxThreshExceeded** notification is not sent until the second address family reaches its maximum route threshold. Routes are not added to the address family that has already reached its maximum route threshold.

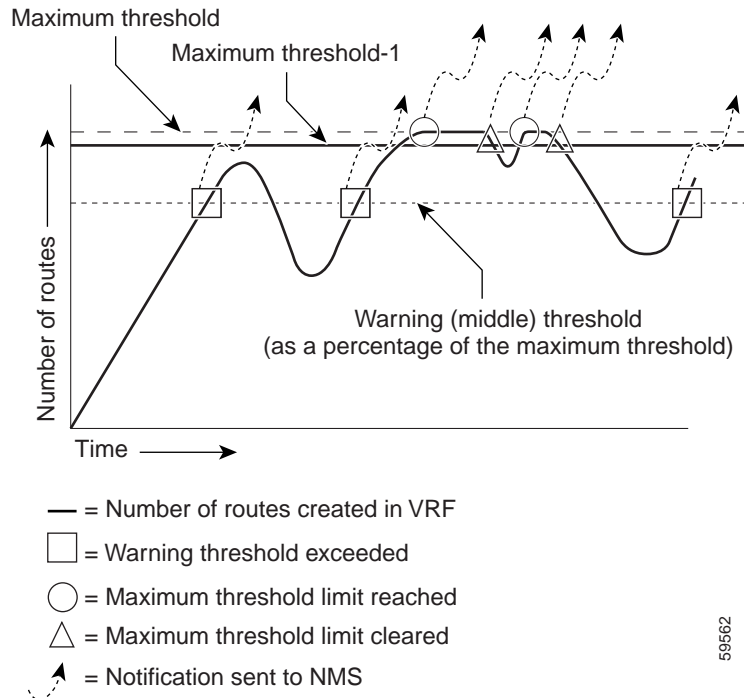


#### Note

If both IPv4 and IPv6 address-family configurations are present in the VRF and one address family does not have a maximum threshold configured, no maximum threshold notification is sent.

- **mplsL3VpnNumVrfSecIlglLblThreshExcd**—This notification is generated and sent when the number of illegal labels received on a VRF interface as indicated by the **mplsL3VpnVrfSecIllegalLblVltns** value has exceeded the **mplsL3VpnIlglLblRcvThresh** value. This threshold is defined with a value of 0. Therefore, a notification is sent when the first illegal label is received on a VRF. Labels are considered illegal if they are outside of the valid label range, do not have a Label Forwarding Information Base (LFIB) entry, or the table ID of the message does not match the table ID for the label in the LFIB.
- **MplsL3VpnNumVrfRouteMaxThreshCleared**—Generated and sent when the number of routes on a VRF attempts to exceed the maximum number of routes and then drops below the maximum number of routes. If you attempt to create a route on a VRF that already contains the maximum number of routes, the **mplsL3VpnVrfNumVrfRouteMaxThreshExceeded** notification is sent (if enabled). When you remove routes from the VRF so that the number of routes falls below the set limit, the **MplsL3VpnNumVrfRouteMaxThreshCleared** notification is sent. You can clear all routes from the VRF by using the **clear ip route vrf** command for IPv4 routes and the **clear ipv6 route vrf** command for IPv6 routes. (See [Figure 6](#) to see when the **MplsL3VpnNumVrfRouteMaxThreshCleared** notification is sent.)



**Figure 6** Comparison of Warning and Maximum Thresholds

For information on the Cisco IOS CLI commands for configuring MPLS-L3VPN-STD-MIB notifications that are sent to an NMS, see the [“How to Configure MPLS EM—MPLS VPN MIB RFC 4382 Upgrade”](#) section on page 30.

## SNMP Notification Specification for the MPLS-L3VPN-STD-MIB

In an SNMPv1 notification, each MPLS Layer 3 VPN notification has a generic type identifier and an enterprise-specific type identifier for identifying the notification type:

- The generic type for all VPN notifications is “enterpriseSpecific” because this is not one of the generic notification types defined for SNMP.
- The enterprise-specific type is identified as follows:
  - 1 for mplsL3VpnVrfUp
  - 2 for mplsL3VpnVrfDown
  - 3 for mplsL3VpnVrfRouteMidThreshExceeded
  - 4 for mplsL3VpnVrfNumVrfRouteMaxThreshExceeded
  - 5 for mplsL3VpnNumVrfSecIllglLblThrshExcd
  - 6 for mplsL3VpnNumVrfRouteMaxThreshCleared

In SNMPv2, the notification type is identified by an SnmpTrapOID varbind (variable binding consisting of an object identifier [OID] type and value) included within the notification message:

- The VRF up and down notifications provide additional variables—mplsL3VpnIfConfRowStatus and mplsL3VpnVrfOperStatus—in the notification. These variables describe the SNMP row status and operational status, respectively.

- The mid threshold notification includes the `mplsL3VpnVrfVConfMidRteThresh` variable and the `mplsL3VpnVrfPerfCurrNumRoutes` variable that indicates the current number of routes within the VRF.
- The max threshold notification includes the `mplsL3VpnVrfVConfHighRteThresh` variable and the `mplsL3VpnVrfPerfCurrNumRoutes` variable that indicates the current number of routes within the VRF.
- The illegal label notification includes the `mplsL3VpnVrfSecIllegalLblVltns` variable that maintains the current count of illegal labels on a VPN.
- The max threshold cleared notification includes the `mplsL3VpnVrfConfHighRteThresh` variable and the `mplsL3VpnVrfPerfCurrNumRoutes` variable that indicates the current number of routes within the VRF.

## MPLS-L3VPN-STD-MIB Notifications Display on Network Management Station

When MPLS-L3VPN-STD-MIB notifications are enabled (see the **snmp-server enable traps mpls rfc vpn** command), notification messages relating to specific MPLS VPN events within Cisco IOS software are generated and sent to a specified NMS in the network. Any utility that supports SNMPv1 or SNMPv2 notifications can receive notification messages.

To monitor MPLS-L3VPN-STD-MIB notification messages, log in to an NMS that supports a utility that displays SNMP notifications, and start the display utility.

## MPLS-L3VPN-STD-MIB Support for IPv6 VPNs over MPLS

The following sections describe how the MPLS-L3VPN-STD-MIB supports IPv6 VPNs over MPLS (6VPE).

- [MPLS-L3VPN-STD-MIB Tables and Objects Support for IPv6 VPNs over MPLS, page 21](#)
- [MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS, page 22](#)
- [Information About Setting Maximum Routes for IPv6 Address-Family VRF Route Limits, page 23](#)

## MPLS-L3VPN-STD-MIB Tables and Objects Support for IPv6 VPNs over MPLS

The MPLS-L3VPN-STD-MIB gets some of the information to populate the MIB objects from the RIB routing table. For the MPLS-L3VPN-STD-MIB to support IPv6 routes over MPLS, the MIB needs to access the RIB routing tables for both IPv6 and IPv4 for the VRF.

[Table 8](#) describes how the MPLS-L3VPN-STD-MIB supports the MIB tables and objects that are specified by address families or that require routing table information.

**Table 8** *MPLS-L3VPN-STD-MIB Support of Address Families in MIB Table and Objects*

MIB Tables and Objects	MPLS-L3VPN-STD-MIB Support
VRF route target table ( <code>mplsL3VpnVrfRTTable</code> )	<p>This table lists the route targets specified for the VRF. For IPv6 VPNs over MPLS, route targets can be specified for each address family.</p> <p>The MPLS-L3VPN-STD-MIB retrieves all route targets for IPv4, then retrieves all route targets specified for IPv6.</p> <p>The <code>mplsL3VpnVrfRTDescr</code> object indicates whether a particular route target was defined in an IPv4 or IPv6 address family.</p>

**Table 8** *MPLS-L3VPN-STD-MIB Support of Address Families in MIB Table and Objects (continued)*

MIB Tables and Objects	MPLS-L3VPN-STD-MIB Support
VRF configuration table (mplsL3VpnVrfTable), mplsL3VpnVrfConfMidRteThresh, mplsL3VpnVrfConfHighRteThresh, mplsL3VpnVrfConfMaxRoutes	<p>The Cisco IOS CLI allows the setting of maximum and middle threshold values on a per-address-family basis.</p> <p>When both IPv4 and IPv6 address-family configurations exist, the MPLS-L3VPN-STD-MIB displays the aggregate value of these settings (not to exceed the max int32 value). If the maximum route limit is configured for one address family and not for the other address family, the aggregate value is max int32 (4,294,967,295).</p> <p>When only a single address-family configuration exists for the VRF, the MPLS-L3VPN-STD-MIB displays the value as configured for the single address family. For more information on how the MPLS-L3VPN-STD-MIB supports notifications, see the <a href="#">“MPLS-L3VPN-STD-MIB Notifications Display on Network Management Station”</a> section on page 21 and the <a href="#">“MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS”</a> section on page 22.</p>
VRF performance table (mplsL3VpnVrfPerfTable), mplsL3VpnVrfPerfRoutesAdded, mplsL3VpnVrfPerfRoutesDeleted, mplsL3VpnVrfPerfCurrNumRoutes, mplsL3VpnVrfPerfRoutesDropped	The MPLS-L3VPN-STD-MIB gets the routing table information from IPv4 and routing table information from IPv6, adds the values, and give a cumulative count for each of the VRF performance table objects.
VRF routing table (mplsL3VpnVrfRteTable)	<p>This table lists the routes associated with this VRF.</p> <p>The MPLS-L3VPN-STD-MIB needs to get all routes from both the IPv4 route table and IPv6 route table for the VRF.</p>
VPN interface configuration table (mplsL3VpnIfConfTable), mplsL3VpnIfVpnRouteDistProtocol	<p>This is a bit mask that indicates the protocol for the interface on which the VRF is defined. The MPLS-L3VPN-STD-MIB needs to get route table information from both the IPv4 address family and the IPv6 address family to look up the protocol and bits to set.</p> <p>This MPLS-L3VPN-STD-MIB information is a union of the IPv4 and IPv6 configurations in the VRF.</p>

## MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS

This section explains how the MPLS-L3VPN-STD-MIB handles the mplsL3VpnVrfRouteMidThreshExceeded, mplsL3VpnVrfNumVrfRouteMaxThreshExceeded, and mplsL3VpnNumVrfRouteMaxThreshCleared notifications.

Notifications for exceeding the route limit for the middle (mplsL3VpnVrfRouteMidThreshExceeded) and maximum (mplsL3VpnVrfNumVrfRouteMaxThreshExceeded) thresholds are triggered by the route table when there is an attempt to add a new route after the number of routes has reached the threshold. With MIB support for both IPv6 and IPv4, two separate route tables could exist for the VRF. When the maximum or middle threshold is exceeded, MPLS-L3VPN-STD-MIB sends notifications to an NMS if you configured these thresholds.

MPLS-L3VPN-STD-MIB manages the maximum and middle thresholds based on an address-family configuration. For Cisco IOS Releases 12.2(33)SRC and 12.2(33)SB, the MPLS-L3VPN-STD-MIB triggers a notification (or trap) based on the aggregate of the IPv4 and IPv6 maximum and middle threshold values.

**Note**

A **maximum** command is introduced in Cisco IOS Release 12.2(33)SRC for the IPv6 address family.

The MPLS-L3VPN-STD-MIB manages the aggregate threshold values as described in the following scenarios:

- Scenario 1: One address family is configured (IPv4 or IPv6); the address family contains maximum and middle threshold configurations:
  - The aggregate max-threshold value is equal to the address family-specific max-route value.
  - The aggregate mid-threshold value is equal to the address family-specific mid-route value.
  - Address family routes stop adding to the routing table when the number of routes reaches the maximum threshold set for the address family. A notification or trap is sent with the next attempt to add a route.
- Scenario 2: Both IPv4 and IPv6 address families are configured; both contain maximum and middle threshold configurations:
  - The aggregate max-threshold value is equal to the sum of the IPv4 and IPv6 max-threshold values (with the upper limit set to a maximum value of 4,294,967,295).
  - The aggregate mid-threshold value is equal to the sum of the IPv4 and IPv6 mid-threshold values. Only when both address families have reached the mid-threshold limit is the notification sent.
  - Address family routes stop adding to the routing table when the number of routes reaches the maximum threshold per address family. A notification or trap is not sent until both IPv4 and IPv6 routes reach the maximum threshold.
- Scenario 3: Both IPv4 and IPv6 address families are configured; only one contains a maximum and middle route threshold configuration:
  - The aggregate max-threshold value is equal to the maximum threshold value (4,294,967,295).
  - The aggregate mid-threshold value is equal to the maximum threshold value (4,294,967,295).
  - Address family routes stop adding to the routing table for the address family that contains the maximum threshold configuration when the number of routes reaches the maximum threshold for the address family. However, no notification or trap is sent.

**Note**

If you configure a single address-family VRF with a maximum and middle threshold (Scenario 1), and later add the other address-family configuration to your VRF without configuring a maximum threshold (Scenario 3), you no longer receive a maximum threshold notification for the original address family when the threshold is reached, but routes would no longer be added to the routing table for this address family.

## Information About Setting Maximum Routes for IPv6 Address-Family VRF Route Limits

You should understand the following before you set maximum routes for the IPv6 address family:

- The **maximum routes** command is entered in address-family configuration mode (the **address-family ipv6** or **address-family ipv4** command) for the specified VRF.
- If you attempt to set the maximum route limit below the current number of routes in the IPv6 routing table for the VRF, the CLI command is rejected. You cannot downsize the IPv6 routing table.

If you configure a warning-only threshold, the command is accepted, but the route limit is not enforced. This statement also applies to IPv4.

- If the routing table has exceeded its route limit, the output from **show ipv6 route vrf** command displays an error message that indicates that the RIB has overflowed.
- If the routing table does not automatically recover from the overflow condition when the number of routes drops below the enforced limit, you would need to enter the **clear ipv6 route vrf** command. This forces the routing table to purge and repopulate.

If the repopulate is successful, then the error condition is cleared. If the automatic or manual purging and repopulate are unsuccessful, the error message in the **show ipv6 route vrf** command output remains.

- For Cisco IOS Releases 12.2(1st)SRC and 12.2(33)SB, the notifications generated in the MPLS-L3VPN-STD-MIB for the route maximum, middle, 3or warnings, and for threshold-cleared objects are an aggregate of the IPv4 and IPv6 route limits and route counts when both routing tables are configured for the VRF.

## MPLS-L3VPN-STD-MIB Data Security

Requirements of the network-facing operator and customers to ensure MPLS-L3VPN-STD-MIB data security are as follows:

- Network-facing operators need to poll all the data in the VRF-aware MPLS-L3VPN-STD-MIB without compromising security. Operators managing the network need to poll all available data in a single SNMP walk.
- Customers managing VRFs from an NMS need to be able to poll data only on VRFs for which they are responsible. Customer VRF information should be visible only to that particular customer. In the configuration example that follows, the customer associated with VRF vrf1 should see only VRF vrf1 information and the customer associated with VRF vrf2 should see only VRF vrf2 information.

Network operators can enter an **snmp-server community** command that contains an access control list (ACL) to make sure that all data is accessible in a single SNMP walk and that customer routers cannot access the data. For example, the operator can enter the following global configuration command: **snmp-server community any-community-name rw access-list acl-number**. The *acl-number* argument can be configured to allow requests from the PE network. This ensures that customer-facing routers cannot access any data using the specified community string.

To ensure that a customer's VRF information is secure, you can configure an SMNP context that is peculiar to the customer's VRF. For example, the following sample configuration ensures that the customer associated with VRF vrf1 and the customer associated with VRF vrf2 both connected to the same PE can access information pertaining only to their own VRF and nothing else:

```
!
vrf definition vrf1
  rd 100:110
  !
  address-family ipv4
    route-target export 100:1000
    route-target import 100:1000
  exit-address-family
!
vrf definition vrf2
  rd 100:120
  !
  address-family ipv4
```

```

route-target export 100:2000
route-target import 100:2000
exit-address-family
!
interface Ethernet3/1
  description Belongs to VPN vrf1
  vrf forwarding vrf1
  ip address 10.20.1.20 255.255.0.0
!
interface Ethernet3/2
  description Belongs to vrf2
  vrf forwarding vrf2
  ip address 10.30.1.10 255.255.0.0
!
access-list 10 permit 10.20.1.21
access-list 10 deny any
access-list 20 permit 10.30.1.11
access-list 20 deny any
!
snmp-server view vrf1View mplsL3VpnMIB.*.*.*.*.3.114.101.100 included
snmp-server view vrf2View mplsL3VpnMIB.*.*.*.*.5.103.114.101.101.110 included
!
snmp-server community vrf1Comm view vrf1View rw 10
snmp-server community vrf2Comm view vrf2View rw 20
!

```

**Note**

The **snmp-server view** commands include mplsL3VpnMIB with OIDs in this format: **mplsL3VpnMIB.\*.\*.\*.\*.length-of-vrf-name.vrf-name-converted-to-octet-character-representation-of-the-name**. For example:

- VRF vrf1 would be represented as 3.114.101.100.
- VRF vrf2 would be represented as 5.103.114.101.101.110.

**Caution**

You should not enter the **snmp-server community *community-name* rw** command unless a firewall protects SNMP requests entered at the PE router. The community string is unprotected and can be used to poll any data from any network.

## Major Differences Between the MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB

The MPLS-L3VPN-STD-MIB based on RFC 4382 provides the same basic functionality as the MPLS-VPN-MIB, draft Version 3 (draft-ietf-ppvpn-mpls-vpn-mib-03.txt). They both provide an interface for MPLS Layer 3 VPNs through the use of SNMP.

After the implementation of the MPLS-L3VPN-STD-MIB (RFC 4382) in Cisco IOS Release 12.2(33)SRC, the MPLS-VPN-MIB will exist for a period of time before support is completely removed. This gives you the chance to migrate to the MPLS-L3VPN-STD-MIB. Both MIBs can coexist in the same image because the MPLS-L3VPN-STD-MIB and the MPLS-VPN-MIB have different root OIDs.

The following sections provide information about the major differences between the MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB:

- [Global Name Changes for the MPLS-L3VPN-STD-MIB Objects, page 26](#)

- [MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Scalar Object Differences, page 26](#)
- [MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Table Object Differences, page 26](#)
- [Tables Not Supported in the MPLS-L3VPN-STD-MIB, page 29](#)
- [MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Notification Differences, page 29](#)

## Global Name Changes for the MPLS-L3VPN-STD-MIB Objects

For the MPLS-L3VPN-STD-MIB, the names of all objects were changed from `mplsVpnname` (MPLS-VPN-MIB object name) to `mplsL3Vpnname`. For example, the VRF configuration table name was changed from `mplsVpnVrfTable` to `mplsL3VpnVrfTable`.

The following sections describe major differences between the MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB objects where the name change is more significant than the global name change.

## MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Scalar Object Differences

[Table 9](#) shows the major difference between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for each scalar object.

**Table 9** *MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Scalar Objects*

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
<code>mplsVpnVrfConfMaxPossibleRoutes</code>	<code>mplsL3VpnVrfConfMaxPossRts</code>	Object name changed.
—	<code>mplsL3VpnVrfConfRteMxThrshTime</code>	New object.
—	<code>mplsL3VpIllLblRcvThrsh</code>	New object.

## MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Table Object Differences

The following tables show the major differences between the MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB objects for each table.

### VRF Configuration Table (`mplsL3VpnVrfTable`)

[Table 10](#) shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VRF configuration table (`mplsL3VpnVrfTable`, formerly `mplsVpnVrfTable`).

**Table 10** *VRF Configuration Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences*

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
—	<code>mplsL3VpnVrfVpnId</code>	New object.
<code>mplsVpnVrfRouteDistinguisher</code>	<code>mplsL3VpnVrfRD</code>	Object name changed.
<code>mplsVpnVrfConfMidRouteThreshold</code>	<code>mplsL3VpnVrfConfMidRteThresh</code>	Object name changed.
<code>mplsVpnVrfConfHighRouteThreshold</code>	<code>mplsL3VpnVrfConfHighRteThresh</code>	Object name changed.
—	<code>mplsL3VpnVrfConfAdminStatus</code>	New object.

**VPN Interface Configuration Table (mplsL3VpnIfConfTable)**

Table 11 shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VPN interface configuration table (mplsL3VpnIfConfTable, formerly mplsVpnInterfaceConfTable).

**Table 11** VPN Interface Configuration Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
mplsVpnInterfaceConfTable	mplsL3VpnIfConfTable	Table name changed.
mplsVpnInterfaceConfIndex	mplsL3VpnIfConfIndex	Object name changed.
mplsVpnInterfaceLabelEdgeType	—	Object deleted.
mplsVpnInterfaceVpnClassification	mplsL3VpnIfVpnClassification	Object name changed.
mplsVpnInterfaceVPNRouteDistProtocol	mplsL3VpnIfVpnRouteDist Protocol	Object name changed.
mplsVpnInterfaceConfStorageType	mplsL3VpnIfConfStorageType	Object name changed.
mplsVpnInterfaceConfRowStatus	mplsL3VpnIfConfRowStatus	Object name changed.

**VRF Route Target Table (mplsL3VpnVrfRTTable)**

Table 12 shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VRF route target table (mplsL3VpnVrfRTTable, formerly mplsVpnVrfRouteTargetTable).

**Table 12** VRF Route Target Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
mplsVpnVrfRouteTargetTable	mplsL3VpnVrfRTTable	Table named changed.
mplsVpnVrfRouteTargetIndex	mplsL3VpnVrfRTIndex	Object name changed.
mplsVpnVrfRouteTargetType	mplsL3VpnVrfRTType	Object name changed.
mplsVpnVrfRouteTarget	mplsL3VpnVrfRT	Object name changed.
mplsVpnVrfRouteTargetDescr	mplsL3VpnVrfRTDescr	Object name changed.
mplsVpnVrfRouteTargetRowStatus	mplsL3VpnVrfRTRowStatus	Object name changed.
—	mplsL3VpnVrfRTStorageType	New object.

**VRF Security Table (mplsL3VpnVrfSecTable)**

Table 13 shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VRF security table (mplsL3VpnVrfSecTable, formerly mplsVpnVrfSecTable).

**Table 13** VRF Security Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
mplsVpnVrfSecIllegalLabelViolations	mplsL3VpnVrfSecIllegalLblVtns	Object name changed.
mplsVpnVrfSecIllegalLabelRcvThresh	—	Object deleted.
—	mplsL3VpnVrfSecDiscontinuityTime	New object.



**VRF Performance Table (mplsL3VpnVrfPerfTable)**

Table 14 shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VRF performance table (mplsL3VpnVrfPerfTable, formerly mplsVpnVrfPerfTable).

**Table 14** VRF Performance Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
—	mplsL3VpnVrfPerfRoutesDropped	New object.
—	mplsL3VpnVrfPerfDiscTime	New object.

**VRF Routing Table (mplsL3VpnVrfRteTable)**

Table 14 shows the major differences between the MPLS-VPN-MIB objects and the MPLS-L3VPN-STD-MIB objects for the VRF routing table (mplsL3VpnVrfRteTable, formerly mplsVpnVrfRouteTable).

The indexing for the VRF routing table has also changed:

- MPLS-VPN-MIB indexing—mplsVpnVrfName, mplsVpnVrfRouteDest, mplsVpnVrfRouteMask, mplsVpnVrfRouteTos, mplsVpnVrfRouteNextHop
- MPLS-L3VPN-STD-MIB indexing—mplsL3VpnVrfName, mplsL3VpnVrfRteInetCidrDestType, mplsL3VpnVrfRteInetCidrDest, mplsL3VpnVrfRteInetCidrPfxLen, mplsL3VpnVrfRteInetCidrPolicy, mplsL3VpnVrfRteInetCidrNHopType, mplsL3VpnVrfRteInetCidrNextHop

**Table 15** VRF Routing Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
mplsVpnVrfRouteTable	mplsL3VpnVrfRteTable	Table name changed.
mplsVpnVrfRouteDest	mplsL3VpnVrfRteInetCidrDest	Object name changed.
mplsVpnVrfRouteDestAddrType	mplsL3VpnVrfRteInetCidrDestType	Object name changed.
mplsVpnVrfRouteMask	—	Object deleted.
mplsVpnVrfRouteMaskAddrType	—	Object deleted.
—	mplsL3VpnVrfRteInetCidrPfxLen	New object.
mplsVpnVrfRouteTos	—	Object deleted.
—	mplsL3VpnVrfRteInetCidrPolicy	New object.
mplsVpnVrfRouteNextHop	mplsL3VpnVrfRteInetCidrNextHop	Object name changed.
mplsVpnVrfRouteNextHopAddrType	mplsL3VpnVrfRteInetCidrNHopType	Object name changed.
mplsVpnVrfRouteIfIndex	mplsL3VpnVrfRteInetCidrIfIndex	Object name changed.
mplsVpnVrfRouteType	mplsL3VpnVrfRteInetCidrType	Object name changed.
mplsVpnVrfRouteProto	mplsL3VpnVrfRteInetCidrProto	Object name changed.
mplsVpnVrfRouteAge	mplsL3VpnVrfRteInetCidrAge	Object name changed.
mplsVpnVrfRouteInfo	—	Object deleted.
mplsVpnVrfRouteNextHopAS	mplsL3VpnVrfRteInetCidrNextHopAS	Object name changed.

**Table 15** VRF Routing Table: MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Object Differences (continued)

MPLS-VPN-MIB Object	MPLS-L3VPN-STD-MIB Object	Difference
mplsVpnVrfRouteMetric1	mplsL3VpnVrfRteInetCidrMetric1	Object name changed.
mplsVpnVrfRouteMetric2	mplsL3VpnVrfRteInetCidrMetric2	Object name changed.
mplsVpnVrfRouteMetric3	mplsL3VpnVrfRteInetCidrMetric3	Object name changed.
mplsVpnVrfRouteMetric4	mplsL3VpnVrfRteInetCidrMetric4	Object name changed.
mplsVpnVrfRouteMetric5	mplsL3VpnVrfRteInetCidrMetric5	Object name changed.
—	mplsL3VpnVrfRteXCPointer	New object.
mplsVpnVrfRouteStatus	mplsL3VpnVrfRteInetCidrStatus	Object name changed.
mplsVpnVrfRouteStorageType	—	Object deleted.

## Tables Not Supported in the MPLS-L3VPN-STD-MIB

The following tables from the MPLS-VPN-MIB are deleted in the MPLS-L3VPN-STD-MIB (RFC 4382):

- BGP neighbor address table (mplsVpnVrfBgpNbrAddrTable)
- BGP neighbor prefix table (mplsVpnVrfBgpNeighborPrefixTable)

The mplsVpnVrfBgpNeighborPrefixTable was not supported in the Cisco IOS implementation of the MPLS-VPN-MIB.

The Cisco-BGP4-MIB based on *Definitions of Managed Objects for BGP-4* (RFC 4273) provides the information related to BGP.

## MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Notification Differences

Table 16 shows the major differences between MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB notifications.

**Table 16** MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Notification Differences

MPLS-VPN-MIB Notification	MPLS-L3VPN-STD-MIB Notification	Difference
mplsVpnVrfIfUp	—	Notification deleted.
mplsVpnVrfIfDown	—	Notification deleted.
—	mplsL3VpnVrfUp	New notification.
—	mplsL3VpnVrfDown	New notification.
mplsNumVrfRouteMidThreshExceeded	mplsL3VpnVrfRouteMidThreshExceeded	Returned objects changed. Notification name change.
mplsNumVrfRouteMaxThreshExceeded	mplsL3VpnVRFNumVrfRouteMaxThreshExceeded	Returned objects changed. Notification name change.

**Table 16** *MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB Notification Differences (continued)*

MPLS-VPN-MIB Notification	MPLS-L3VPN-STD-MIB Notification	Difference
mplsNumVrfSecIllegalLabelThreshExceeded	mplsL3VpnNumVrfSecIllegalLblThreshExcd	Returned objects changed. Notification name change.
cMplsNumVrfRouteMaxThreshCleared (from the CISCO-IETF-PPVPN-MPLS-VPN-MIB)	mplsL3VpnNumVrfRouteMaxThreshCleared	Notification name changed.

## How to Configure MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

This section contains tasks to configure the MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature. The MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature introduces the MPLS-L3VPN-STD-MIB. Perform the following tasks to configure your router to use SNMP to monitor and manage MPLS Layer 3 VPNs:

- [Configuring the SNMP Community, page 30](#) (required)
- [Configuring the Router to Send MPLS Layer 3 VPN SNMP Notifications to a Host, page 32](#) (optional)
- [Configuring Threshold Values for MPLS Layer 3 VPN SNMP Notifications, page 35](#) (optional)
- [Configuring SMNP Controls for MPLS Layer 3 VPN Notification Thresholds: Examples, page 39](#) (optional)

### Configuring the SNMP Community

The SNMP agent for the MPLS-L3VPN-STD-MIB is disabled by default and must be enabled for you to use SNMP for monitoring and managing MPLS Layer 3 VPNs on your network.

An SNMP community string defines the relationship between the SNMP manager and the agent. The community string acts like a password to regulate access to the agent on the router.

Perform this task to configure an SNMP community.

#### SUMMARY STEPS

1. **enable**
2. **show running-config**
3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [*acl-number*]
5. **do copy running-config startup-config**
6. **exit**
7. **show running-config** | **include** *[option]*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration to determine if an SNMP agent is already running.  If no SNMP information is displayed, continue with the next step.  If any SNMP information is displayed, you can modify the information or change it as needed.
Step 3	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 4	<b>snmp-server community</b> <i>string</i> [ <b>view</b> <i>view-name</i> ] [ <b>ro</b>   <b>rw</b> ] [ <i>acl-number</i> ]  <b>Example:</b> Router(config)# snmp-server community comaccess ro	Configures the community access string to permit access to the SNMP protocol. <ul style="list-style-type: none"> <li>The <i>string</i> argument acts like a password and permits access to the SNMP protocol.</li> <li>The <b>view</b> <i>view-name</i> keyword and argument pair specifies the name of a previously defined view. The view defines the objects available to the community.</li> <li>The <b>ro</b> keyword specifies read-only access. Authorized management stations are able to retrieve only MIB objects.</li> <li>The <b>rw</b> keyword specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.</li> <li>The <i>acl-number</i> argument is an integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.</li> </ul>
Step 5	<b>do copy running-config startup-config</b>  <b>Example:</b> Router(config)# do copy running-config startup-config	Saves the modified configuration to NVRAM as the startup configuration file. <ul style="list-style-type: none"> <li>The <b>do</b> command allows you to perform EXEC-level commands in configuration mode.</li> </ul>

	Command or Action	Purpose
Step 6	<b>exit</b>  <b>Example:</b> Router(config)# exit	Returns to privileged EXEC mode.
Step 7	<b>show running-config   include [option]</b>  <b>Example:</b> Router# show-running config   include snmp-server	(Optional) Displays the configuration information currently on the router, the configuration for a specific interface, or map-class information.  <ul style="list-style-type: none"> <li>Use the <b>show running-config</b> command to confirm that the <b>snmp-server</b> statements appear in the output.</li> </ul>

## Configuring the Router to Send MPLS Layer 3 VPN SNMP Notifications to a Host

Perform this task to configure the router to send MPLS Layer 3 VPN SNMP notifications or traps to a host.

The **snmp-server host** command specifies which hosts receive the notifications. The **snmp-server enable traps** command globally enables the trap production mechanism for the specified notifications.

For a host to receive a notification, an **snmp-server host** command must be configured for that host, and, generally, the notification must be enabled globally through the **snmp-server enable traps** command.



### Note

Although you can set the *community-string* argument using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server host** *host-addr* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] [**vrf** *vrf-name*]
4. **snmp-server enable traps mpls rfc vpn** [**illegal-label**] [**max-thresh-cleared**] [**max-threshold**] [**mid-threshold**] [**vrf-down**] [**vrf-up**]
5. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>snmp-server host</b> <i>host-addr</i> [<b>traps</b>   <b>informs</b>] [<b>version</b> {<b>1</b>   <b>2c</b>   <b>3</b> [<b>auth</b>   <b>noauth</b>   <b>priv</b>]}] <i>community-string</i> [<b>udp-port</b> <i>port</i>] [<i>notification-type</i>] [<b>vrf</b> <i>vrf-name</i>]</p> <p><b>Example:</b> Router(config)# snmp-server host 172.20.2.160 traps comaccess mpls-vpn</p>	<p>Specifies the recipient of an SNMP notification operation.</p> <ul style="list-style-type: none"> <li>The <i>host-addr</i> argument specifies the name or Internet address of the host (the targeted recipient).</li> <li>The <b>traps</b> keyword sends SNMP traps to this host. This is the default.</li> <li>The <b>informs</b> keyword sends SNMP informs to this host.</li> <li>The <b>version</b> keyword specifies the version of the SNMP used to send the traps. Version 3 is the most secure model, because it allows packet encryption with the <b>priv</b> keyword. If you use the <b>version</b> keyword, you must specify one of the following: <ul style="list-style-type: none"> <li><b>1</b> —SNMPv1. This option is not available with informs.</li> <li><b>2c</b> —SNMPv2C.</li> <li><b>3</b> —SNMPv3. The following three optional keywords can follow the <b>version 3</b> keyword: <b>auth</b>, <b>noauth</b>, <b>priv</b>.</li> </ul> </li> <li>The <i>community-string</i> argument is a password-like community string sent with the notification operation.</li> <li>The <b>udp-port</b> <i>port</i> keyword and argument pair names the User Datagram Protocol (UDP) port of the host to use. The default is 162.</li> <li>The <i>notification-type</i> argument specifies the type of notification to be sent to the host. If no type is specified, all notifications are sent.</li> <li>The <b>vrf</b> <i>vrf-name</i> keyword and argument pair specifies the VRF table that should be used to send SNMP notifications.</li> </ul>

Command or Action	Purpose
<p><b>Step 4</b></p> <pre>snmp-server enable traps mpls rfc vpn [illegal-label] [max-thresh-cleared] [max-threshold] [mid-threshold] [vrf-down] [vrf-up]</pre> <p><b>Example:</b></p> <pre>Router(config)# snmp-server enable traps mpls rfc vpn vrf-down vrf-up</pre>	<p>Enables the router to send MPLS Layer 3 VPN-specific SNMP notifications (traps and informs).</p> <ul style="list-style-type: none"> <li>The <b>illegal-label</b> keyword enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have an LFIB entry, or do not match table IDs for the label.</li> <li>The <b>max-thresh-cleared</b> keyword enables a notification when the number of routes falls below the limit after the maximum route limit was attempted.</li> </ul> <p><b>Note</b> For information on notifications if a VRF has both IPv4 and IPv6 address-family configurations, see the <a href="#">“MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS”</a> section on page 22.</p> <ul style="list-style-type: none"> <li>The <b>max-threshold</b> keyword enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another <code>mplsL3VpnVrfNumVrfRouteMaxThreshExceeded</code> notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. The max-threshold value is determined by the <b>maximum routes</b> command in VRF configuration mode.</li> </ul> <p><b>Note</b> For more information on the maximum threshold notification if both IPv4 and IPv6 address family configurations are present in the VRF, see the <a href="#">“MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS”</a> section on page 22.</p> <ul style="list-style-type: none"> <li>The <b>mid-threshold</b> keyword enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.</li> </ul> <p><b>Note</b> For more information on the maximum threshold notification if both IPv4 and IPv6 address family configurations are present in the VRF, see the <a href="#">“MPLS-L3VPN-STD-MIB Notifications Support for IPv6 VPNs over MPLS”</a> section on page 22.</p> <ul style="list-style-type: none"> <li>The <b>vrf-down</b> keyword enables a notification when the last interface in a VRF goes from the up state to the down state.</li> <li>The <b>vrf-up</b> keyword enables a notification when all interfaces in a VRF are previously in a down state and one VRF interface goes to the up state.</li> </ul>

	Command or Action	Purpose
Step 5	<pre>end</pre> <p><b>Example:</b>  <pre>Router(config)# end</pre></p>	(Optional) Exits to privileged EXEC mode.

## Configuring Threshold Values for MPLS Layer 3 VPN SNMP Notifications

Perform this task to configure the following threshold values for MPLS Layer 3 VPN SNMP notifications:

- The `mplsL3VpnVrfRouteMidThreshExceeded` notification event is generated and sent when the middle threshold (warning) is crossed. You can configure this threshold in the CLI by using the **maximum routes** command in VRF configuration mode. This notification is sent to the NMS only at the time the threshold is exceeded. Whenever the number of routes falls below this threshold and exceeds the threshold again, a notification is sent to the NMS.

If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the warning threshold values. An `mplsL3VpnVrfRouteMidThreshExceeded` notification is not sent until the second address family reaches its warning threshold.

- The `mplsL3VpnVrfNumVrfRouteMaxThreshExceeded` notification event is generated and sent when you attempt to create a route on a VRF that already contains the maximum number of routes as defined by the **maximum routes** command in VRF configuration mode. A trap notification is sent to the NMS when you attempt to exceed the maximum threshold. Another `mplsL3VpnVrfNumVrfRouteMaxThreshExceeded` notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again.

If both IPv4 and IPv6 address-family configurations are present in the VRF, the threshold is an aggregate of the maximum threshold values. An `mplsL3VpnVrfNumVrfRouteMaxThreshExceeded` notification is not sent until the second address family reaches its maximum route threshold. Routes are not added to the address family that has already reached its maximum route threshold.

See [Figure 6](#) for an example of how this notification works and for a comparison of the maximum and warning thresholds.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family** {*ipv4* | *ipv6*}
5. **maximum routes** *limit warn-threshold*  
or  
**maximum routes** *limit warn-only*
6. **exit-address-family**
7. **end**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>vrf definition</b> <i>vrf-name</i>  <b>Example:</b> Router(config)# vrf definition vpn1	Configures a VRF routing table and enters VRF configuration mode. <ul style="list-style-type: none"> <li>The <i>vrf-name</i> argument specifies the name assigned to a VRF.</li> </ul>
Step 4	<b>address-family</b> { <i>ipv4</i>   <i>ipv6</i> }  <b>Example:</b> Router(config-vrf) address-family ipv4	Enters VRF address family configuration mode. <ul style="list-style-type: none"> <li>The <b>ipv4</b> keyword specifies an address family for an IPv4 VPN.</li> <li>The <b>ipv6</b> keyword specifies an address family for an IPv6 VPN.</li> </ul>
Step 5	<b>maximum routes</b> <i>limit</i> <i>warn-threshold</i>  <b>Example:</b> Router(config-vrf-af)# maximum routes 10000 80 or <b>maximum routes</b> <i>limit</i> <b>warn-only</b>  <b>Example:</b> Router(config-vrf-af)# maximum routes 10000 warn-only	Limits the maximum number of routes in a VRF to prevent a PE router from importing too many routes. <ul style="list-style-type: none"> <li>The <i>limit</i> argument specifies the maximum number of routes allowed in a VRF. The range is from 1 to 4,294,967,295.</li> <li>The <i>warn-threshold</i> argument generates a warning when the number of routes set by the <i>warn-threshold</i> argument is reached and rejects routes that exceed the maximum number set in the <i>limit</i> argument. The warning threshold is a percentage from 1 to 100 of the maximum number of routes specified in the <i>limit</i> argument.</li> <li>The <b>warn-only</b> keyword specifies that a system message logging (syslog) error message is issued when the maximum number of routes allowed for a VRF exceeds the limit threshold. However, additional routes are still allowed.</li> </ul>
Step 6	<b>exit-address-family</b>  <b>Example:</b> Router(config-vrf-af)# exit-address-family	Exits from VRF address family configuration mode.
Step 7	<b>end</b>  <b>Example:</b> Router(config-vrf)# end	(Optional) Exits to privileged EXEC mode.

## Configuring SNMP Controls for MPLS VPN Notification Thresholds

Perform this task to configure the following SNMP controls for MPLS VPN notification thresholds:

- The `mplsL3VpnVrfConfRteMxThrshTime` is the interval at which the maximum route exceeded notification (`mplsL3VpnVrfNumVrfRouteMaxThreshExceeded`) is reissued after the maximum value is exceeded (or reached) and after the initial notification was sent. You can configure this interval in the CLI by using the **`snmp mib mpls vpn max-threshold`** *seconds* command in global configuration mode. Configure this command if you want to receive more than the initial notification that the maximum route value is exceeded.
- The `mplsL3VpnNumVrfSecIlglLblThrshExcd` notification is generated and sent when the number of illegal label violations on a VRF has exceeded the number indicated by the `mplsL3VpnIlglLblRcvThrsh` scalar. You can configure the number of illegal labels that generate the `mplsL3VpnNumVrfSecIlglLblThrshExcd` notification in the CLI by using the **`snmp mib mpls vpn illegal-label`** *number* command in global configuration mode. Configure this command if you want to allow a certain number of illegal label violations before you receive the `mplsL3VpnNumVrfSecIlglLblThrshExcd` notification.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **`snmp mib mpls vpn max-threshold`** *seconds*
4. **`snmp mib mpls vpn illegal-label`** *number*
5. **end**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b><code>snmp mib mpls vpn max-threshold</code></b> <i>seconds</i>	Configures SNMP controls for MPLS VPN notification thresholds.
	<b>Example:</b> Router(config)# snmp mib mpls vpn max-threshold 3600	<ul style="list-style-type: none"> <li>• The <b><code>max-threshold</code></b> keyword controls MPLS VPN maximum threshold exceeded notifications.</li> <li>• The <i>seconds</i> argument is the time in seconds before SNMP resends maximum threshold notifications. The valid range is from 0 to 4,294,967,295. The default is 0.</li> </ul>

	Command or Action	Purpose
Step 4	<pre>snmp mib mpls vpn illegal-label number</pre> <p><b>Example:</b>  Router(config)# snmp mib mpls vpn illegal-label 10</p>	<p>Configures simple SNMP controls for MPLS VPN notification thresholds.</p> <ul style="list-style-type: none"> <li>The <b>illegal-label</b> keyword controls MPLS VPN illegal label threshold exceeded notifications.</li> <li>The <i>number</i> argument is the number of illegal labels allowed before SNMP sends an illegal label threshold notification. The valid range is from 1 to 4,294,967,295. The default is 0.</li> </ul>
Step 5	<pre>end</pre> <p><b>Example:</b>  Router(config)# end</p>	<p>Exits to privileged EXEC mode.</p>

## Configuration Examples for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

This section contains the following configuration examples for the MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature:

- [Configuring the SNMP Community: Examples, page 38](#)
- [Configuring the Router to Send MPLS Layer 3 VPN SNMP Traps: Example, page 39](#)
- [Configuring Threshold Values for MPLS Layer 3 VPN SNMP Notifications: Examples, page 39](#)
- [Configuring SMNP Controls for MPLS Layer 3 VPN Notification Thresholds: Examples, page 39](#)

### Configuring the SNMP Community: Examples

The following example shows enabling a simple SNMP community group. This configuration permits any SNMP client to access all MPLS-L3VPN-STD-MIB objects with read-only access using the community string comaccess.

```
configure terminal
!
snmp-server community comaccess ro
```

Use the following command to verify that the SNMP master agent is enabled for the MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature:

```
Router# show running-config | include snmp-server
```

```
Building configuration...
....
snmp-server community comaccess RO
....
```



#### Note

If you do not see any “snmp-server” statements, SNMP is not enabled on the router.

## Configuring the Router to Send MPLS Layer 3 VPN SNMP Traps: Example

The following example shows you how to enable the router to send MPLS Layer 3 VPN notifications to host 172.20.2.160 using the comaccess community string if a VRF transitions from an up or down state:

```
configure terminal
!
snmp-server host 172.20.2.160 traps comaccess mpls-vpn
snmp-server enable traps mpls rfc vpn vrf-down vrf-up
```

## Configuring Threshold Values for MPLS Layer 3 VPN SNMP Notifications: Examples

The following example shows how to set a maximum threshold of 10,000 routes and a warning threshold that is 80 percent of the maximum threshold for a VRF named vpn1 on a router:

```
configure terminal
!
vrf definition vpn1
 address-family ipv4
  maximum routes 10000 80
 exit address-family
end
```

The following example shows how to set a warning threshold of 10,000 routes for a VRF named vpn2 on a router. An error message is generated; however, additional routes are still allowed because a maximum route threshold is not set with this command.

```
configure terminal
!
vrf definition vpn2
 address-family ipv4
  maximum routes 10000 warn-only
 exit address-family
end
```

## Configuring SNMP Controls for MPLS Layer 3 VPN Notification Thresholds: Examples

The following examples show how to configure SNMP controls for MPLS Layer 3 VPN notification thresholds.

In this example, an interval of 2 hours (7200 seconds) is configured for the resending of maximum threshold exceeded notifications after the first notification was sent and the attempt to add routes continues:

```
configure terminal
!
snmp mib mpls vpn max-threshold 7200
end
```

If you do not configure an interval to resend maximum route exceeded notifications, SNMP sends a single maximum threshold notification at the time that the maximum threshold is exceeded.

In the following example, the number of illegal labels allowed for a VRF is configured as 5 before SNMP sends an illegal label threshold exceeded notification:

## Additional References

```
configure terminal
!
snmp mib mpls vpn illegal-label 5
end
```

If you do not configure an illegal label threshold, then SNMP sends an illegal label notification on the first occurrence of an illegal label.

## Additional References

The following sections provide references related to the MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature.

## Related Documents

Related Topic	Document Title
Configuration tasks and information about MPLS Layer 3 VPNs	<a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a>
Configuration tasks and information about IPv6 VPNs over MPLS	<a href="#">“Implementing IPv6 VPN over MPLS (6VPE)” chapter in the Cisco IOS IPv6 Configuration Library</a>
Description of commands related to Cisco IPv6	<a href="#">Cisco IOS IPv6 Command Reference</a>
Descriptions of and links to other MPLS Layer 3 VPN feature documentation	<a href="#">Cisco IOS Multiprotocol Label Switching Configuration Guide</a>
Description of commands related to MPLS Layer 3 VPNs	<a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>

## Standards

Standard	Title
<a href="http://www.rfc-editor.org/rfc/rfc2578.txt">http://www.rfc-editor.org/rfc/rfc2578.txt</a>	<i>Structure of Management Information Version 2 (SMIv2)</i>

## MIBs

MIB	MIBs Link
MPLS-L3VPN-STD-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2578	<i>Structure of Management Information Version 2 (SMIv2)</i>
RFC 2685	<i>Virtual Private Networks Identifier</i>
RFC 2863	<i>The Interfaces Group MIB</i>
RFC 3031	<i>Multiprotocol Label Switching Architecture</i>
RFC 3410	<i>Introduction and Applicability Statements for the Internet-Standard Management Framework</i>
RFC 3413	<i>Simple Network Management Protocol (SNMP) Applications</i>
RFC 3813	<i>Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB)</i>
RFC 4001	<i>Textual Conventions for Internet Network Addresses</i>
RFC 4273	<i>Definitions of Managed Objects for BGP-4</i>
RFC 4364	<i>BGP/MPLS IP Virtual Private Networks (VPNs)</i>
RFC 4382	<i>MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **maximum routes**
- **snmp mib mpls vpn**
- **snmp-server enable traps mpls rfc vpn**

# Feature Information for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

Table 17 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 17 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 17** Feature Information for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade

Feature Name	Releases	Feature Information
MPLS EM—MPLS VPN MIB RFC 4382 Upgrade	12.2(33)SRC 12.2(33)SB	<p>The MPLS EM—MPLS VPN MIB RFC 4382 Upgrade feature document describes the MIB that supports Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) based on RFC 4382, <i>MPLS/BGP Virtual Private Network (VPN) Management Information Base</i>. This document also describes the differences between RFC 4382 and the MPLS-VPN-MIB based on the Internet Engineering Task Force (IETF) draft Version 3 (draft-ietf-ppvpn-mpls-vpn-mib-03.txt) and describes the changes needed to implement MPLS-L3VPN-STD-MIB (RFC 4382). The MPLS-VPN-MIB and MPLS-L3VPN-STD-MIB provide an interface for managing the MPLS VPN feature in Cisco IOS software through the use of the Simple Network Management Protocol (SNMP).</p> <p>Cisco IOS MPLS Embedded Management (EM) is a set of standards and value-added services that facilitate the deployment, operation, administration, and management of MPLS-based networks according to the fault, configuration, accounting, performance, and security (FCAPS) model.</p> <p>In 12.2(33)SRC, this feature was introduced on the Cisco 7600 series router.</p> <p>In 12.2(33)SB, the feature was implemented for the Cisco 10000 series router on the Cisco 10000 Performance Routing Engine 2 (PRE-2) and PRE-3.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">MPLS Layer 3 VPN Overview, page 3</a></li> </ul>



**Table 17**      **Feature Information for MPLS EM—MPLS VPN MIB RFC 4382 Upgrade (continued)**

Feature Name	Releases	Feature Information
		<ul style="list-style-type: none"> <li>• <a href="#">MPLS-L3VPN-STD-MIB Benefits</a>, page 3</li> <li>• <a href="#">Capabilities Supported by the MPLS-L3VPN-STD-MIB</a>, page 3</li> <li>• <a href="#">Supported Objects in the MPLS-L3VPN-STD-MIB</a>, page 4</li> <li>• <a href="#">MPLS-L3VPN-STD-MIB Scalar Objects</a>, page 5</li> <li>• <a href="#">MPLS-L3VPN-STD-MIB MIB Tables</a>, page 6</li> <li>• <a href="#">MPLS-L3VPN-STD-MIB Notification Events</a>, page 18</li> <li>• <a href="#">MPLS-L3VPN-STD-MIB Support for IPv6 VPNs over MPLS</a>, page 21</li> <li>• <a href="#">MPLS-L3VPN-STD-MIB Data Security</a>, page 24</li> <li>• <a href="#">Major Differences Between the MPLS-VPN-MIB and the MPLS-L3VPN-STD-MIB</a>, page 25</li> <li>• <a href="#">Configuring the SNMP Community</a>, page 30</li> <li>• <a href="#">Configuring the Router to Send MPLS Layer 3 VPN SNMP Notifications to a Host</a>, page 32</li> <li>• <a href="#">Configuring Threshold Values for MPLS Layer 3 VPN SNMP Notifications</a>, page 35</li> </ul> <p>The following commands were introduced or modified:  <b>maximum routes</b>, <b>snmp mib mpls vpn</b>, <b>snmp-server enable traps mpls rfc vpn</b>.</p>

# Glossary

**6VPE router**—Provider edge router that provides BGP-MPLS IPv6 VPN service over an IPv4-based MPLS core. It is a IPv6 VPN PE, dual-stack router that implements 6PE concepts on the core-facing interfaces.

**autonomous system**—A collection of networks that share the same routing protocol and that are under the same system administration.

**ASN.1**—Abstract Syntax Notation One. The data types independent of particular computer structures and representation techniques. Described by ISO International Standard 8824.

**BGP**—Border Gateway Protocol. The exterior Border Gateway Protocol used to exchange routing information between routers in separate autonomous systems. BGP uses TCP. Because TCP is a reliable protocol, BGP does not experience problems with dropped or fragmented data packets.

**BGP prefixes**—A route announcement using the BGP. A prefix is composed of a path of autonomous system numbers, indicating which networks the packet must pass through, and the IP block that is being routed. A BGP prefix would look something like: 701 1239 42 206.24.14.0/24. (The /24 part is referred to as a CIDR mask.) The /24 indicates that there are 24 ones in the netmask for this block starting from the left side. A /24 corresponds to the natural mask 255.255.255.0.

**CE router**—customer edge router. A router on the border between a VPN provider and a VPN customer that belongs to the customer.

**CIDR**—classless interdomain routing. A technique supported by BGP4 and based on route aggregation. CIDR allows routers to group routes to reduce the quantity of routing information carried by the core routers. With CIDR, several IP networks appear to networks outside the group as a single, larger entity. With CIDR, IP addresses and their subnet masks are written as four octets, separated by periods, followed by a forward slash and a two-digit number that represents the subnet mask.

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. Cisco Express Forwarding optimizes network performance and scalability for networks with large and dynamic traffic patterns.

**community**—In SNMP, a logical group of managed devices and NMSs in the same administrative domain.

**community name**—*See* community string.

**community string**—A text string that acts as a password and is used to authenticate messages sent between a managed station and a router containing an SNMP agent. The community string is sent in every packet between the manager and the client. Also called a community name.

**IETF**—Internet Engineering Task Force. A task force consisting of over 80 working groups responsible for developing Internet standards. The IETF operates under the auspices of ISOC. *See also* ISOC.

**informs**—A type of notification message that is more reliable than a conventional trap notification message, because the informs message notification requires acknowledgment, and a trap notification does not.

**ISOC**—Internet Society. An international nonprofit organization, founded in 1992, that coordinates the evolution and use of the Internet. In addition, ISOC delegates authority to other groups related to the Internet, such as the IAB. ISOC is headquartered in Reston, Virginia (United States).

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**LDP**—Label Distribution Protocol. A standard protocol between MPLS-enabled routers that is used for the negotiation of the labels (addresses) used to forward packets.

**LFIB**—Label Forwarding Information Base. In the Cisco Label Switching system, the data structure for storing information about incoming and outgoing tags (labels) and associated equivalent packets suitable for labeling.

**LSR**—label switch router. A device that forwards MPLS packets based on the value of a fixed-length label encapsulated in each packet.

**MIB**—Management Information Base. A database of network management information that is used and maintained by a network management protocol such as SNMP or CMIP. The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**MPLS interface**—An interface on which MPLS traffic is enabled.

**MPLS VPN**—Multiprotocol Label Switching Virtual Private Network. An IP network infrastructure delivering private network services over a public infrastructure using a Layer 3 backbone. Using MPLS VPNs in a Cisco IOS network provides the capability to deploy and administer scalable Layer 3 VPN backbone services including applications, data hosting network commerce, and telephony services to business customers.

For an MPLS VPN solution, an MPLS VPN is a set of provider edge routers that are connected by means of a common “backbone” network to supply private IP interconnectivity between two or more customer sites for a given customer. Each VPN has a set of provisioning templates and policies and can span multiple provider administrative domains (PADs).

**NMS**—network management system. A powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**notification**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred. *See also* trap.

**PE router**—provider edge router. A router on the border between a VPN provider and a VPN customer that belongs to the provider.

**QoS**—quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

**RIB**—Routing Information Base. Also called the routing table.

**RT**—route target. An extended community attribute that identifies a group of routers and, in each router of that group, a subset of forwarding tables maintained by the router that can be populated with a BGP route carrying that extended community attribute. The RT is a 64-bit value by which Cisco IOS software discriminates routes for route updates in VRFs.

**SNMP**—Simple Network Management Protocol. The network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security. *See also* SNMP2.

**SNMP2**—SNMP Version 2. Version 2 of the popular network management protocol. SNMP2 supports centralized and distributed network management strategies, and includes improvements in the Structure of Management Information (SMI), protocol operations, management architecture, and security. *See also* SNMP.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps (notifications) are less reliable than inform requests, because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received. *See also* notification.

**VPN**—Virtual Private Network. A group of sites that, as the result of a set of administrative policies, are able to communicate with each other over a shared backbone network. A VPN is a secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone. *See also* MPLS VPN.

**VPN ID**—A mechanism that identifies a VPN based on RFC 2685. A VPN ID consists of an Organizational Unique Identifier (OUI), a three-octet hex number assigned by the IEEE Registration Authority, and a VPN index, a four-octet hex number, which identifies the VPN within the company.

**VRF**—VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)

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

© 2008 Cisco Systems, Inc. All rights reserved.





# Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

---

**First Published: August 25, 2004**

**Last Updated: February 27, 2009**

The Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services feature provides Simple Network Management Protocol (SNMP) support within an Any Transport over Multiprotocol Label Switching (AToM) infrastructure emulating Ethernet, Frame Relay, and ATM services over packet switched networks (PSNs). The Pseudowire Emulation Edge-to-Edge (PWE3) MIBs are the following:

- CISCO-IETF-PW-MIB (PW-MIB)
- CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB)
- CISCO-IETF-PW-ENET-MIB (PW-ENET-MIB)
- CISCO-IETF-PW-FR-MIB (PW-FR-MIB)
- CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB)

Cisco IOS Release 12.2(28)SB introduces support for the CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB), which provides network management information specific to an ATM over pseudowire connection in a Multiprotocol Label Switching (MPLS) AToM or an IP network.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services”](#) section on page 28.

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



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 2](#)
- [Restrictions for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 2](#)
- [Information About Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 3](#)
- [How to Configure Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 20](#)
- [Configuration Examples for the Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 24](#)
- [Additional References, page 25](#)
- [Command Reference, page 27](#)
- [Feature Information for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services, page 28](#)
- [Glossary, page 30](#)

## Prerequisites for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

- SNMP must be enabled on the label switch routers (LSRs).
- MPLS must be enabled on the LSRs.
- Pseudowires must be configured with Ethernet, Frame Relay, or ATM access circuits. (For more detailed information, see the [Any Transport over MPLS](#), [Configuring Frame Relay](#), and [Configuring ATM](#) feature modules.

## Restrictions for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

The PWE3 MIBs are limited to read-only (RO) permission for MIB objects except for the cpwVcUp and cpwVcDown notification enable object, cpwVcUpDownNotifEnable, which has been extended to be writable by the SNMP agent.

- The following tables in the PW-MIB are not supported:
  - cpwVcPerfCurrentTable
  - cpwVcPerfIntervalTable
- The following objects in the PW-MPLS-MIB are not supported:
  - cpwVcMplsOutboundIndexNext
  - cpwVcMplsInboundIndexNext
- The following tables in the PW-ENET-MIB are not supported:

- cpwVcEnetMplsPriMappingTable
  - cpwVcEnetStatsTable
- The following table in the PW-FR-MIB is not supported:
  - cpwVcFrPMTTable
- The PW-ATM-MIB does not support cell counters on the Cisco 7500 series router. Consequently, an SNMP query for cell counters returns a 0 value.
- The PW-ATM-MIB does not support a high-capacity cell counter per virtual path (VP) or cells per port.
- The PW-ATM-MIB virtual path identifier (VPI)/virtual channel identifier (VCI) value for port mode cell relay is 0.
- The PW-ATM-MIB VP cell relay VCI value is 0.
- The PW-ATM-MIB VP does not support ATM adaptation layer 5 (AAL5); therefore, all packet counters are invalid.

**Note**

This feature is not supported over Ethernet, Frame Relay, and ATM in all releases. See the [“Feature Information for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services”](#) section on page 28 for more detailed information.

## Information About Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

To configure the Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services feature, you should understand the following concepts:

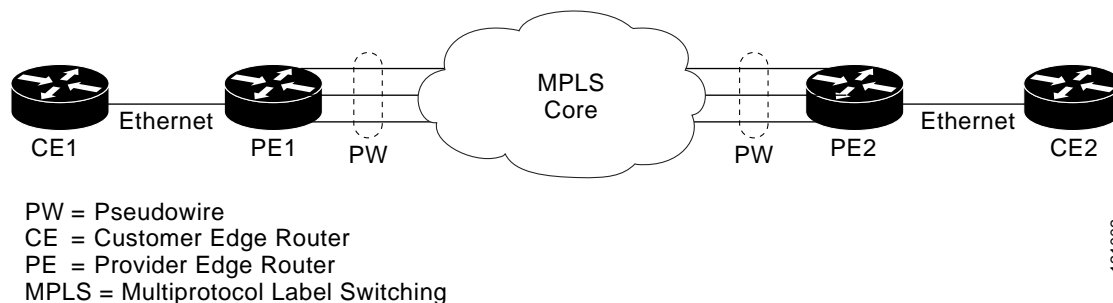
- [The Function of a Pseudowire in the PWE3 MIBs, page 4](#)
- [PWE3 MIBs Architecture, page 4](#)
- [Components and Functions of the PWE3 MIBs, page 5](#)
- [Tables in the PW-MIB, page 6](#)
- [Tables in the PW-MPLS-MIB, page 12](#)
- [Tables in the PW-ENET-MIB, page 16](#)
- [Tables in the PW-FR-MIB, page 17](#)
- [Tables in the PW-ATM-MIB, page 17](#)
- [Objects in the PWE3 MIBs, page 19](#)
- [Scalar Objects in the PWE3 MIBs, page 19](#)
- [Notifications in the PWE3 MIBs, page 20](#)
- [Benefits of the PWE3 MIBs, page 20](#)



## The Function of a Pseudowire in the PWE3 MIBs

A pseudowire is a point-to-point connection between pairs of provider edge (PE) routers (as shown in Figure 1). Its primary function is to emulate services like Ethernet over an underlying core MPLS network through encapsulation into a common MPLS format. By encapsulating services into a common MPLS format, a pseudowire allows carriers to converge their services to an MPLS network.

**Figure 1** Sample Pseudowire Topology

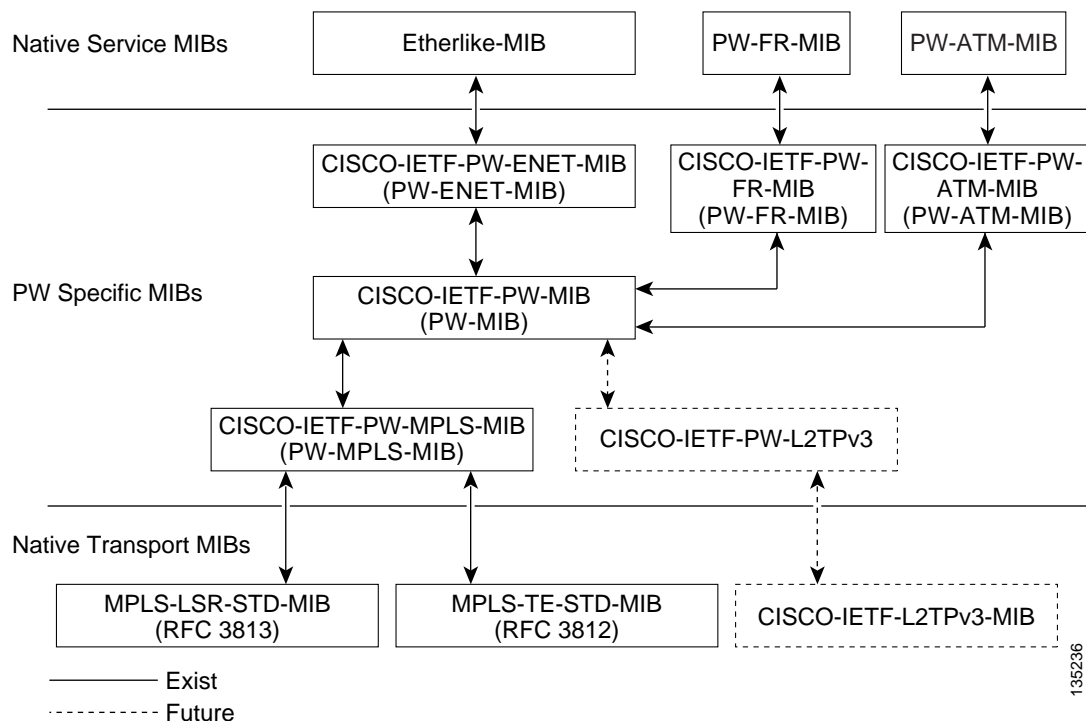


121002

## PWE3 MIBs Architecture

The PWE3 MIBs architecture shown in Figure 2 categorizes three groups of MIBs that, when used together, provide the complete emulated service; the native transport, which carries the service across the core network; and the relationship between the two.

**Figure 2** PWE3 MIBs Architecture



135236

The architecture is modular in that once deployed, new emulated service MIB modules or additional transport MIB modules “plug in” to or extend the existing infrastructure rather than require a new and unique one. This allows you to build management applications without the concern of a new service requiring the deployment of a completely different management strategy. Because the architecture is a generalized association mechanism between existing service and transport MIB modules, native MIB modules work in the absence of the associated PWE3-specific MIBs. The advantage is that if a PWE3-specific MIB has not yet been deployed in Cisco IOS software, which associates a service or transport with pseudowires, these MIB modules can still be queried. However, the only drawback is that the associations with the pseudowires are absent.

## Components and Functions of the PWE3 MIBs

The PWE3 MIBs have the following components and functions:

- PW-MIB (the pseudowire MIB)

This MIB binds the PW-MPLS-MIB and the PW-ENET-MIB together, and provides status of the pseudowire emulation and statistics and configuration information. The PW-MIB also defines the notifications for pseudowire fault and event monitoring.

- PW-MPLS-MIB (the pseudowire MPLS-MIB)

This MIB contains managed objects that can be used by a network manager to monitor pseudowire emulation MPLS services, such as MPLS-traffic engineering (TE)-PSN and MPLS-non-TE-PSN.

This MIB shows the following:

- Cross-connect (XC) indexes for virtual circuits (VCs) that are Label Distribution Protocol (LDP)-signaled and have a preferred path that is not set to an MPLS TE tunnel.
- Tunnel indexes for VCs with a preferred path set to a TE tunnel and an output interface that is a TE tunnel.

- PW-ENET-MIB (the pseudowire Ethernet services MIB)

This MIB contains managed objects that can be used by a network manager to monitor pseudowire emulation Ethernet services.

- PW-FR-MIB (the pseudowire Frame Relay services MIB)

This MIB contains managed objects that can be used by a network manager to monitor pseudowire emulation Frame Relay services.

This MIB uses a Frame Relay over pseudowire (FRoPW) connection that consists of two segments: the Frame Relay segment and the pseudowire segment. The PW-FR-MIB provides hooks to those segments. The PW MIB contains information about the pseudowire segment, and the PW-FR-MIB contains information about the Frame Relay segment.

The PW-FR-MIB is defined at the Pseudowire Service Emulation Layer and resides on top of the generic PW-MIB as shown in [Figure 2](#). Therefore, the PW-FR-MIB is highly dependent on the existence and the service provided by the PW-MIB. In addition, an existing PW-FR connection entry must associate with an existing VC entry in the PW-MIB.

The PW-FR-MIB and the generic PW-MIB are logically tied by the PW VC Index, which is an internal index defined to support the PW-MIB. Each PW VC index uniquely maps into an existing VC entry in the PW-MIB and the PW-FR-MIB.

- PW-ATM-MIB (the pseudowire ATM services MIB)

This MIB contains managed objects that can be used by a network manager to monitor pseudowire emulation ATM services.

This MIB uses an ATM over pseudowire (ATMoPW) connection that consists of two segments: the ATM segment and the pseudowire segment. The PW-ATM-MIB provides hooks to those segments. The PW MIB contains information about the pseudowire segment, and the PW-ATM-MIB contains information about the ATM segment called the attachment circuit.

The PW-ATM-MIB is defined at the Pseudowire Service Emulation Layer and resides on top of the generic PW-MIB as shown in [Figure 2](#). Therefore, the PW-ATM-MIB is highly dependent on the existence and the service provided by the PW-MIB. In addition, an existing PW-ATM connection entry must associate with an existing VC entry in the PW-MIB.

The PW-ATM-MIB and the generic PW-MIB are logically tied by the PW VC Index, which is an internal index defined to support the PW-MIB. Each PW VC index uniquely maps into an existing VC entry in the PW-MIB and the PW-ATM-MIB.

## Tables in the PW-MIB

The PW-MIB consists of the following tables:

- **cpwVcTable** ([Table 1](#))—Contains high-level generic parameters related to VC creation. This table is implemented as read only and is indexed by the `cpwVcIndex`, which uniquely identifies a singular connection. A row in this table represents an emulated virtual connection. This table is used for all VC types.
- **cpwVcPerfTotalTable** ([Table 2](#))—Provides per-VC performance information from the VC start time. This table is indexed by the `cpwVcIndex`.
- **cpwVcIdMappingTable** ([Table 3](#))—Provides reverse mapping of the existing VCs based on VC type and VC ID ordering. This table is typically useful for element manager software (EMS) ordered query of existing VCs. This table is indexed by `cpwVcIdMappingVcType`, `cpwVcIdMappingVcID`, `cpwVcIdMappingPeerAddrType`, and `cpwVcIdMappingPeerAddr`. This table is implemented as read only.
- **cpwVcPeerMappingTable** ([Table 4](#))—Provides reverse mapping of the existing VCs based on VC type and VC ID ordering. This table is typically useful for EMS ordered query of existing VCs. This table is indexed by `cpwVcPeerMappingPeerAddrType`, `cpwVcPeerMappingPeerAddr`, `cpwVcPeerMappingVcType`, and `cpwVcPeerMappingVcID`. This table is implemented as read only.

### cpwVcTable

[Table 1](#) lists the `cpwVcTable` objects and their descriptions.

**Table 1** *cpwVcTable Objects and Descriptions*

Objects	Description
cpwVcType	Indicates the service to be carried over this VC. This is circuit type information.
cpwVcOwner	Set by the operator to indicate the protocol responsible for establishing this VC. Values are the following: <ul style="list-style-type: none"> <li>• manual(1)—Used when no maintenance protocol (PW signaling) is needed to set up the VC, such as configuration of entries in the VC tables including VC labels, and so forth.</li> <li>• maintenanceProtocol(2)—Used for standard signaling of the VC for the specific PSN; for example, LDP for MPLS PSN as specified in <i>draft-martini-l2circuit-trans-mpls</i> or the Layer 2 Tunneling Protocol (L2TP).</li> <li>• other(3)—Used for all other types of signaling.</li> </ul>
cpwVcPsnType	Set by the operator to indicate the PSN type on which this VC is carried. Based on this object, the relevant PSN table entries are created in the PSN-specific MIB modules. For example, if mpls(1) is defined, the agent creates an entry in the cpwVcMplsTable, which further defines the MPLS PSN configuration.
cpwVcSetUpPriority	Defines the relative setup priority of the VC in a lowest-to-highest manner, where 0 is the highest priority. This value is significant if there are competing resources between VCs and the implementation supports this feature. Because this is not implemented in AToM, the value of 0 is used.
cpwVcHoldingPriority	Defines the relative holding priority of the VC in a lowest-to-highest manner, where 0 is the highest priority. This value is significant if there are competing resources between VCs and the implementation supports this feature. Because this is not implemented in AToM, the value of 0 is used.
cpwVcInboundMode	Enables greater security for implementations that use per-platform VC label space. Modes are the following: <ul style="list-style-type: none"> <li>• strict(1)</li> <li>• loose(2)</li> </ul> <p>In strict mode, packets coming from the PSN are accepted only from tunnels that are associated to the same VC via the inbound tunnel table in the case of MPLS, or as identified by the source IP address in the case of L2TP or IP PSN. The entries in the inbound tunnel table are either explicitly configured or implicitly known by the maintenance protocol used for VC setup.</p> <p>If such association is not known, not configured, or not desired, loose mode should be configured, and the node should accept the packet based on the VC label only, regardless of the outer tunnel used to carry the VC.</p>

**Table 1** *cpwVcTable Objects and Descriptions (continued)*

<b>Objects</b>	<b>Description</b>
cpwVcPeerAddrType	Denotes the address type of the peer node maintenance protocol (signaling) address if the PW maintenance protocol is used for the VC creation. It should be set to unknown if the PW maintenance protocol is not used; for example, cpwVcOwner is set to manual.
cpwVcPeerAddr	Contains the value of the peer node address of the PW maintenance protocol entity. This object should contain a value of 0 if not relevant (manual configuration of the VC).
cpwVcID	Use in the outgoing VC ID field within the VC forward equivalence class (FEC) element with LDP signaling or the PW ID attribute-value (AV) pair for the L2TP.
cpwVcLocalGroupID	Use in the Group ID field sent to the peer PW within the maintenance protocol for VC setup; 0 if not used.
cpwVcControlWord	Defines if the control word is sent with each packet by the local node.
cpwVcLocalIfMtu	If not = 0, the optional IfMtu object in the maintenance protocol is sent with this value, representing the locally supported maximum transmission unit (MTU) size over the interface (or the virtual interface) associated with the VC.
cpwVcLocalIfString	Each VC is associated to an interface (or a virtual interface) in the ifTable of the node as part of the service configuration. This object defines if the maintenance protocol sends the interface's name as it appears in the ifTable in the name object as part of the maintenance protocol. If this object is set to false, the optional element is not sent.
cpwVcRemoteGroupID	Obtained from the Group ID field as received via the maintenance protocol used for VC setup; 0 if not used. The value of 0xFFFF is used if the object is not defined by the VC maintenance protocol.
cpwVcRemoteControlWord	If the maintenance protocol is used for VC establishment, this parameter indicates the received status of the control word usage; that is, if packets are received with the control word or not. The value of notYetKnown is used while the maintenance protocol has not yet received the indication from the remote node. In a manual configuration of the VC, this parameter indicates to the local node the expected encapsulation for the received packets.
cpwVcRemoteIfMtu	The remote interface MTU as received from the remote node via the maintenance protocol. This object should be 0 if this parameter is not available or not used.
cpwVcRemoteIfString	Indicates the interface description string as received by the maintenance protocol; it must be a NULL string if not applicable or not known yet.

**Table 1** *cpwVcTable Objects and Descriptions (continued)*

<b>Objects</b>	<b>Description</b>
cpwVcOutboundVcLabel	The VC label used in the outbound direction toward the PSN. This object may be set up manually if the owner is manual; otherwise, it is automatic. Examples; for MPLS PSN, the label represents the 20 bits of the VC tag; for L2TP, it represents the 32 bits of the session ID. If the label is not yet known (signaling in process), the object should return a value of 0xFFFF.
cpwVcInboundVcLabel	The VC label used in the inbound direction for packets received from the PSN. This object may be set up manually if the owner is manual; otherwise, it is automatic. Examples; for MPLS PSN, the label represents the 20 bits of VC tag; for L2TP, the label represents the 32 bits of the session ID. If the label is not yet known (signaling in process), the object should return a value of 0xFFFF.
cpwVcName	The canonical name assigned to the VC.
cpwVcDescr	A textual string containing information about the VC. If there is no description, this object contains a 0 length string.
cpwVcCreateTime	System time when this VC was created.
cpwVcUpTime	Number of consecutive ticks that this VC has been up in both directions together. (Up is observed in cpwVcOperStatus.)
cpwVcAdminStatus	The desired operational status of this VC.
cpwVcOperStatus	Indicates the actual combined operational status of this VC. This object is up if both cpwVcInboundOperStatus and cpwVcOutboundOperStatus are in the up state. For all other values, if the VCs in both directions are of the same value, this object reflects that value; otherwise, it is set to the more severe status of the two. The order of severity from most severe to less severe is as follows: unknown, notPresent, down, lowerLayerDown, dormant, testing, and up. The operator can consult the direction of OperStatus for fault isolation.
cpwVcInboundOperStatus	Indicates the actual operational status of this VC in the inbound direction. Values are the following: <ul style="list-style-type: none"> <li>up—The VC is established and ready to pass packets.</li> <li>down—PW signaling has not yet finished or indications available at the service level show that the VC is not passing packets.</li> <li>testing—AdminStatus at the VC level is set to test.</li> <li>dormant—The VC is not available because the required resources are occupied by higher priority VCs.</li> <li>notPresent—Some component needed for the setup of the VC is missing.</li> <li>lowerLayerDown—The underlying PSN is not in OperStatus up.</li> </ul>

**Table 1** *cpwVcTable Objects and Descriptions (continued)*

Objects	Description
cpwVcOutboundOperStatus	<p>Indicates the actual operational status of this VC in the outbound direction. Values are the following:</p> <ul style="list-style-type: none"> <li>• up—The VC is established and ready to pass packets.</li> <li>• down—PW signaling has not yet finished or indications available at the service level show that the VC is not passing packets.</li> <li>• testing—AdminStatus at the VC level is set to test.</li> <li>• dormant—The VC is not available because the required resources are occupied by higher priority VCs.</li> <li>• notPresent—Some component needed for the setup of the VC is missing.</li> <li>• lowerLayerDown—The underlying PSN is not in OperStatus up.</li> </ul>
cpwVcTimeElapsed	<p>The number of seconds, including partial seconds, that have elapsed since the beginning of the current measurement period. If, for some reason, such as an adjustment in the system's time-of-day clock, and the current interval exceeds the maximum value, the agent returns the maximum value. Because cpwVcPerfIntervalTable is not implemented, this is 0.</p>
cpwVcValidIntervals	<p>The number of previous 15-minute intervals for which data was collected. An agent with PW capability must be capable of supporting at least <math>x</math> intervals. The minimum value of <math>x</math> is 4; the default of <math>x</math> is 32, and the maximum value of <math>x</math> is 96. The value is <math>x</math> unless the measurement was (re)started within the last <math>x \times 15</math> minutes, in which case the value will be the number of complete 15-minute intervals; for example, in the case where the agent is a proxy, some intervals may be unavailable. In this case, this interval is the maximum interval number for which data is available. This interval is set to 0.</p>
cpwVcRowStatus	<p>A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.</p>
cpwVcStorageType	<p>The storage type for this object is a read-only implementation that is always volatile(2).</p>

## cpwVcPerfTotalTable

Table 2 lists the cpwVcPerfTotalTable objects and their descriptions.

**Table 2** *cpwVcPerfTotalTable Objects and Descriptions*

Objects	Description
cpwVcPerfTotalInHCPackets	High-capacity counter for the number of packets received by the VC from the PSN.
cpwVcPerfTotalInHCBytes	High-capacity counter for the number of bytes received by the VC from the PSN.
cpwVcPerfTotalOutHCPackets	High-capacity counter for the number of packets forwarded by the VC to the PSN.
cpwVcPerfTotalOutHCBytes	High-capacity counter for the number of bytes forwarded by the VC (to the PSN).
cpwVcPerfTotalDiscontinuityTime	The value of sysUpTime on the most recent occasion when one or more of this object's counters suffered a discontinuity. The relevant counters are the specific instances of any Counter32 or Counter64. If no such discontinuities have occurred since the last reinitialization of the local management subsystem, this object contains a 0 value.

## cpwVcIdMappingTable

Table 3 lists the cpwVcIdMappingTable objects and their descriptions.

**Table 3** *cpwVcIdMappingTable Objects and Descriptions*

Objects	Description
cpwVcIdMappingVcType	The VC type (indicates the service) of this VC.
cpwVcIdMappingVcID	The VC ID of this VC; 0 if the VC is configured manually.
cpwVcIdMappingPeerAddrType	IP address type of the peer node.
cpwVcIdMappingPeerAddr	IP address of the peer node.
cpwVcIdMappingVcIndex	The value that represents the VC in the cpwVcTable.

## cpwVcPeerMappingTable

Table 4 lists the cpwVcPeerMappingTable objects and their descriptions.

**Table 4** *cpwVcPeerMappingTable Objects and Descriptions*

Objects	Description
cpwVcPeerMappingPeerAddrType	IP address type of the peer node.
cpwVcPeerMappingPeerAddr	IP address of the peer node.
cpwVcPeerMappingVcType	The VC type (indicates the service) of this VC.
cpwVcPeerMappingVcID	The VC ID of this VC; 0 if the VC is configured manually.
cpwVcPeerMappingVcIndex	The value that represents the VC in the cpwVcTable.



## Tables in the PW-MPLS-MIB

The PW-MPLS-MIB consists of the following tables:

- **cpwVcMplsTable** ([Table 5](#))—Specifies information for the VC to be carried over an MPLS PSN. This table is indexed on `cpwVcIndex`.
- **cpwVcMplsOutboundTable** ([Table 6](#))—Associates VCs using an MPLS PSN with the outbound MPLS tunnels toward the PSN or the physical interface in the case of the VC only. A row in this table represents a link between PW VCs that require MPLS tunnels and an MPLS tunnel toward the PSN. This table is indexed by the `cpwVcIndex` and an additional index that is not supported; consequently, its value is 1. The operator creates at least one entry in this table for each PW VC that requires an MPLS PSN. The VC-only case and the `cpwVcMplsOutboundIndex` is not supported.
- **cpwVcMplsInboundTable** ([Table 7](#))—Associates VCs using an MPLS PSN with the inbound MPLS tunnels for packets coming from the PSN, if such association is desired mainly for security reasons. A row in this table represents a link between PW VCs that require MPLS tunnels and an MPLS tunnel for packets arriving from the PSN. This table is indexed by the set of indexes used to identify the VC, `cpwVcIndex`, and an additional index that is not supported; consequently, its value is 1. An entry is created in this table either automatically by the local agent or manually by the operator when strict mode is required. This table points to the appropriate MPLS MIB. For MPLS-TE, the four variables relevant to the indexing of an MPLS TE tunnel are set. The VC-only case and the `cpwVcMplsInboundIndex` are not supported.
- **cpwVcMplsNonTeMappingTable** ([Table 8](#))—Maps an inbound or outbound tunnel to a VC in non-TE applications. A row in this table represents the association between a PW VC and its non-TE MPLS outer tunnel. An application can use this table to retrieve the PW carried over a specific non-TE MPLS outer tunnel quickly. This table is indexed by the `xconnect` index for the MPLS non-TE tunnel and the direction of the VC in the specific entry. The same table is used in both inbound and outbound directions, but in a different row for each direction. If the inbound association is not known, no rows should exist for it. Rows are created by the local agent when all the association data is available for display.
- **cpwVcMplsTeMappingTable** ([Table 9](#))—Maps an inbound or outbound tunnel to a VC in MPLS-TE applications. A row in this table represents the association between a PW VC and its MPLS-TE outer tunnel. An application can use this table to retrieve the PW carried over a specific TE MPLS outer tunnel quickly. This table is indexed by the four indexes of a TE tunnel, the direction of the VC specific entry, and the `VcIndex`. The same table is used in both inbound and outbound directions, but a different row for each direction. If the inbound association is not known, no rows should exist for it. Rows are created by the local agent when all the association data is available for display. This table shows mappings between pseudowires and the `xconnect` index for non-TE outer tunnel or index.

### cpwVcMplsTable

[Table 5](#) lists the `cpwVcMplsTable` objects and their descriptions.

**Table 5** *cpwVcMplsTable Objects and Descriptions*

Objects	Description
cpwVcMplsMplsType	Set by the operator to indicate the outer tunnel types, if they exist. Values are the following: <ul style="list-style-type: none"> <li>mplsTe(0)—Used when the outer tunnel is set up by MPLS-TE.</li> <li>mplsNonTe(1)—Used when the outer tunnel is set up by LDP or manually.</li> </ul>
cpwVcMplsExpBitsMode	Set by the operator to indicate the way the VC shim label EXP bits are to be determined. The value is the following: <ul style="list-style-type: none"> <li>outerTunnel(1)—Used when there is an outer tunnel and cpwVcMplsMplsType is mplsTe or mplsNonTe.</li> </ul>
cpwVcMplsExpBits	Set by the operator to indicate the MPLS EXP bits to be used on the VC shim label if cpwVcMplsExpBitsMode is specified; value = 0.
cpwVcMplsTtl	Set by the operator to indicate the VC time-to-live (TTL) bits to be used on the VC shim label; value = 0.
cpwVcMplsLocalLdpID	The local LDP identifier of the LDP entity creating this VC in the local node. Because the VC labels are always set from the per-platform label space, the last two octets in the LDP ID must be 0s.
cpwVcMplsLocalLdpEntityID	The local LDP entity index of the LDP entity to be used for this VC on the local node; this should be set to all 0s when this object is not used.
cpwVcMplsPeerLdpID	The peer LDP identifier as identified by the LDP session; this should be zero if not relevant or not known yet.
cpwVcMplsStorageType	The storage type for this object is a read-only implementation that is always volatile(2).

## cpwVcMplsOutboundTable

Table 6 lists the cpwVcMplsOutboundTable objects and their descriptions.

**Table 6** *cpwVcMplsOutboundTable Objects and Descriptions*

Objects	Description
cpwVcMplsOutboundIndex	An arbitrary index for enabling multiple rows per VC in this table. The next available free index can be retrieved using cpwVcMplsOutboundIndexNext. The value = 1, because this object is not supported.
cpwVcMplsOutboundLsrXcIndex	Set by the operator. If the outer label is defined in the MPL-LSR-MIB, that is, set by LDP or manually, this object points to the xconnect index of the outer tunnel. Otherwise, this object is set to 0.

**Table 6** *cpwVcMplsOutboundTable Objects and Descriptions (continued)*

Objects	Description
cpwVcMplsOutboundTunnelIndex	Part of the set of indexes for an outbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, this object is set to 0.
cpwVcMplsOutboundTunnelInstance	Part of the set of indexes for an outbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, this object is set to 0.
cpwVcMplsOutboundTunnelLclLSR	Part of the set of indexes for an outbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, this object is set to NULL.
cpwVcMplsOutboundTunnelPeerLSR	Part of the set of indexes for an outbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, this object is set to NULL.
cpwVcMplsOutboundIfIndex	For a VC only with no outer tunnel, this object holds the ifIndex of the outbound port. The value = 0.
cpwVcMplsOutboundRowStatus	A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.
cpwVcMplsOutboundStorageType	The storage type for this object is a read-only implementation that is always volatile(2).

## cpwVcMplsInboundTable

Table 7 lists the cpwVcMplsInboundTable objects and their descriptions.

**Table 7** *cpwVcMplsInboundTable Objects and Descriptions*

Objects	Description
cpwVcMplsInboundIndex	An arbitrary index for enabling multiple rows per VC in this table. The next available free index can be retrieved using cpwVcMplsInboundIndexNext. the value = 1, because this object is not supported.
cpwVcMplsInboundLsrXcIndex	If the outer label is defined in the MPL-LSR-MIB; that is, set by LDP or manually, this object points to the xconnect index of the outer tunnel. The xconnect index represents the pseudowire in the inbound direction retrieving 0 if information for this object is not known.
cpwVcMplsInboundTunnelIndex	Part of the set of indexes for an inbound tunnel, specifically an MPLS-TE outer tunnel; value = 0. This object does not support TE tunnels at the ingress router.
cpwVcMplsInboundTunnelInstance	Part of the set of indexes for an inbound tunnel, specifically an MPLS-TE outer tunnel; value = 0. This object does not support TE tunnels at the ingress router.
cpwVcMplsInboundTunnelLclLSR	Part of the set of indexes for an inbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, set to NULL. This object does not support TE tunnels at the ingress router.

**Table 7** *cpwVcMplsInboundTable Objects and Descriptions (continued)*

Objects	Description
cpwVcMplsInboundTunnelPeerLSR	Part of the set of indexes for an inbound tunnel, specifically an MPLS-TE outer tunnel; otherwise, this object is set to NULL. This object does not support TE tunnels at the ingress router.
cpwVcMplsInboundIfIndex	In the case of a VC only (no outer tunnel), this object holds the ifIndex of the inbound port. The value = 0.
cpwVcMplsInboundRowStatus	A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.
cpwVcMplsInboundStorageType	The storage type for this object is a read-only implementation that is always volatile(2).

## cpwVcMplsNonTeMappingTable

Table 8 lists the cpwVcMplsNonTeMappingTable objects and their descriptions.

**Table 8** *cpwVcMplsNonTeMappingTable Objects and Descriptions*

Objects	Description
cpwVcMplsNonTeMappingTunnelDirection	Identifies if the row represents an outbound or inbound mapping.
cpwVcMplsNonTeMappingXcTunnelIndex	XC index in the MPLS-LSR-MIB of the pseudowire LDP-generated XC entry.
cpwVcMplsNonTeMappingIfIndex	Identifies the port on which the VC is carried for VC only; the value = 0.
cpwVcMplsNonTeMappingVcIndex	Represents the VC in the cpwVcTable.

## cpwVcMplsTeMappingTable

Table 9 lists the cpwVcMplsTeMappingTable objects and their descriptions.

**Table 9** *cpwVcMplsTeMappingTable Objects and Descriptions*

Objects	Description
cpwVcMplsTeMappingTunnelDirection	Identifies if the row represents an outbound mapping.
cpwVcMplsTeMappingTunnelIndex	Index for the conceptual row identifying an MPLS-TE tunnel.
cpwVcMplsTeMappingTunnelInstance	Identifies an instance of an MPLS-TE tunnel.
cpwVcMplsTeMappingTunnelPeerLsrID	Identifies a peer LSR when the outer tunnel is MPLS-TE based.
cpwVcMplsTeMappingTunnelLocalLsrID	Identifies the local LSR.
cpwVcMplsTeMappingVcIndex	Represents the VC in the cpwVcTable.

## Tables in the PW-ENET-MIB

The PW-ENET-MIB consists of the following table:

- **cpwVcEnetTable** ([Table 10](#))—Provides Ethernet port mapping and VLAN configuration for each Ethernet emulated virtual connection. This table is indexed on **cpwVcIndex**, which uniquely identifies a singular connection. The second level index for this table is **cpwVcEnetPwVlan**, which indicates VLANs on this VC. This table is used only for Ethernet VC types—**ethernetVLAN**, **ethernet**, or **ethernet virtual private LAN service (VPLS)**, and is implemented as read-only.

### cpwVcEnetTable

[Table 10](#) lists the **cpwVcEnetTable** objects and their descriptions.

**Table 10** *cpwVcEnetTable Objects and Descriptions*

Objects	Description
<b>cpwVcEnetPwVlan</b>	The VLAN value for frames on a VC. This is one of the indexes to the table so multiple VLAN values can be configured for a PW VC. This value is 4096 to indicate untagged frames; that is, if the <b>cpwVcEnetVlanMode</b> value is <b>removeVlan</b> . This value is the VLAN value of the access circuit if the <b>cpwVcEnetVlanMode</b> value is <b>noChange</b> . The value of 4097 is used if the object is not applicable; for example, when mapping all packets from an Ethernet port to the VC.
<b>cpwVcEnetVlanMode</b>	Indicates the way the VLAN field is handled between the access circuit and the PW VC. The possible values for this field are as follows: <ul style="list-style-type: none"> <li>• <b>noChange</b>—Indicates that the VC contains the original user VLAN, as specified in <b>cpwVcEnetPortVlan</b>.</li> <li>• <b>changeVlan</b>—Indicates that the VLAN field on the VC may be different from the VLAN field on the user's port.</li> <li>• <b>removeVlan</b>—Indicates that the encapsulation on the VC does not include the original VLAN field.</li> </ul>
<b>cpwVcEnetPortVlan</b>	Defines the VLAN value on the physical port (or VPLS virtual port) if a change is required to the VLAN value between the VC and the physical or virtual port. It is equal to <b>cpwVcEnetPwVlan</b> if the <b>cpwVcEnetVlanMode</b> value is <b>noChange</b> . A value of 4096 indicates that no VLAN is associated with the VC; that is, assigning Default VLAN to untagged frames. If all traffic from the VC is being forwarded to the port, then this value is 4097 indicating it is not relevant.
<b>cpwVcEnetPortIfIndex</b>	The <b>ifIndex</b> value of the Ethernet port associated with this PW VC for point-to-point Ethernet service. For VPLS, this value is an <b>ifIndex</b> value for a virtual interface for the VPLS instance.

**Table 10** *cpwVcEnetTable Objects and Descriptions (continued)*

Objects	Description
cpwVcEnetVcIfIndex	Models the VC as a virtual interface in the ifTable. This value is always 0 to indicate no virtual interface is created.
cpwVcEnetRowStatus	A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.
cpwVcEnetStorageType	The storage type for this object is a read-only implementation that is always volatile(2).

## Tables in the PW-FR-MIB

The PW-FR-MIB consists of the following table:

- cpwVcFrTable ([Table 11](#))—Contains entries that represent an FRoPW connection operating in one-to-one mapping mode in which there is a one-to-one correspondence between a Frame Relay VC and a pair of unidirectional pseudowires.

### cpwVcFrTable

[Table 11](#) lists the cpwVcFrTable objects and their descriptions.

**Table 11** *cpwVcFrTable Objects and Descriptions*

Objects	Description
cpwVcFrIfIndex	Returns the interface ifIndex of the Frame Relay (FR) segment of the FRoPW connection.
cpwVcFrDlci	Returns the data-link connection identifier (DLCI) of the Frame Relay segment of an FRoPW connection.
cpwVcFrAdminStatus	Returns the administrative status of an FRoPW connection.
cpwVcFrOperStatus	Returns the combined operational status of an FRoPW connection.
cpwVcFrPw2FrOperStatus	Returns the operational status of the PW-to-FR direction in an FRoPW connection.
cpwVcFrRowStatus	A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.
cpwVcFrStorageType	The storage type for this object is a read-only implementation that is always volatile(2).

## Tables in the PW-ATM-MIB

The PW-ATM-MIB consists of the following tables:

- cpwVcAtmTable ([Table 12](#))—Specifies information for an ATM VC to be carried over the PSN.
- cpwVcAtmPerfTable ([Table 13](#))—Specifies performance-related attributes for an ATM VC.

## cpwVcAtmTable

Table 12 lists the cpwVcAtmTable objects and their descriptions.

**Table 12** *cpwVcAtmTable Objects and Descriptions*

Objects	Description
cpwAtmIf	Specifies the ATM interface that sends and receives cells from the ATM network.
cpwAtmVpi	Specifies the VPI value of the ATM VC.
cpwAtmVci	Specifies the VCI value of the ATM VC.
cpwAtmClpQosMapping	Indicates the presence of cell loss priority (CLP) bits determining the value in quality of service (QoS) fields of the encapsulating protocol. The value could be used only for outbound traffic, which means traffic going out to the PSN.
cpwAtmRowStatus	A read-only implementation that is always active(1). It is used for creating, modifying, and deleting.
cpwAtmOamCellSupported	Indicates whether operation, administration, and maintenance (OAM) cells are transported on this VC.
cpwAtmQosScalingFactor	Represents the scaling factor to be applied to ATM QoS rates when calculating QoS rates for the PSN domain.
cpwAtmCellPacking	Identifies if the VC is configured to do cell packing.
cpwAtmMncp	Identifies the number of cells that need to be packed.
cpwAtmEncap	Provides information on whether MPLS or Layer 2 Tunneling Protocol Version 3 (L2TPv3) is used as the transport.
cpwAtmPeerMncp	Represents the maximum number of cells that can be packed in one packet for a peer interface.
cpwAtmMcptTimeout	Represents the maximum cell packing timeout (MCPT) value used.

## cpwVcAtmPerfTable

Table 13 lists the cpwVcAtmPerfTable objects and their descriptions.

**Table 13** *cpwVcAtmPerfTable Objects and Descriptions*

Objects	Description
cpwAtmCellsReceived	Obtains information on the number of cells that were received and sent to the PSN.
cpwAtmCellsSent	Provides information on the number of cells sent to the ATM network.
cpwAtmCellsRejected	Indicates the number of cells that were rejected by this VC because of policing.
cpwAtmCellsTagged	Indicates the number of cells that were tagged.

**Table 13** *cpwVcAtmPerfTable Objects and Descriptions (continued)*

Objects	Description
cpwAtmHCCellsReceived	Provides the high-capacity counter for the number of cells received by this VC.
cpwAtmHCCellsRejected	Provides the high-capacity counter for the number of cells rejected by this VC.
cpwAtmHCCellsTagged	Provides the high-capacity counter for number of cells that were tagged.
cpwAtmAvgCellsPacked	Provides the average number of cells that were packed.
cpwAtmPktsReceived	Indicates the number of ATM AAL5 packets that are actually sent into the ATM network as packets when the VC is configured to do AAL5 over PW.
cpwAtmPktsSent	Gets the number of packets that are reconstructed from the cells, assigns a VC label, and sends the packets into the PSN.
cpwAtmPktsRejected	Indicates the number of packets that were rejected because of policing.

## Objects in the PWE3 MIBs

The PWE3 MIBs represent an ASN.1 notation reflecting specific components of the pseudowire services. The MIBs enable a network management application using SNMP to get this information for display. The MIBs support the standard GETNEXT and GETBULK functionality, but do not support configuration capabilities (via SET) in the current implementation.

## Scalar Objects in the PWE3 MIBs

The PWE3 MIBs contain the following supported scalar object:

- **cpwVcUpDownNotifEnable**—This object reflects the configuration of the cpwVcUp and cpwVcDown notifications. If either of the notifications is configured via the command-line interface (CLI), then this object has a value of true(1). If this object is set via SNMP to true(1), then it enables the emission of both the cpwVcUp and cpwVcDown notifications; if the object is set via SNMP to false(2), these notifications are not emitted.



### Note

cpwVcUpDownNotifEnable can be set only if RW is configured for the **snmp-server community string [view view-name] [ro | rw] [ipv6 nacl] [access-list-number]** command.

The PWE3 MIBs contain the following unsupported scalar objects:

- **cpwVcIndexNext**—Indicates the next cpwVcIndex value to use when you add rows to the cpwVcTable.
- **cpwVcNotifRate**—Indicates the rate at which cpwVcUp/Down notifications can be issued from the device.
- **cpwVcMplsOutboundIndexNext**—Contains an appropriate value to be used for cpwVcMplsOutboundIndex when you create entries in the cpwVcMplsOutboundTable. The value 0 indicates that no unassigned entries are available. To obtain the cpwVcMplsOutboundIndex value



for a new entry, the manager issues a management protocol retrieval operation to obtain the current value of this object. After each retrieval, the software agent should modify the value to the next unassigned index; however, the software agent *must not* assume such retrieval will be done for each row created.

- **cpwVcMplsInboundIndexNext**—Contains an appropriate value to be used for **cpwVcMplsInboundIndex** when you create entries in the **cpwVcMplsInboundTable**. The value 0 indicates that no unassigned entries are available. To obtain the **cpwVcMplsInboundIndex** value for a new entry, the manager issues a management protocol retrieval operation to obtain the current value of this object. After each retrieval, the software agent should modify the value to the next unassigned index; however, the agent *must not* assume such retrieval will be done for each row created.

## Notifications in the PWE3 MIBs

The **cpwVcUp** and **cpwVcDown** notifications in the PW-MIB indicate when the **operStatus** values for a range of PW VCs have changed state.

The definition of these objects in the PW-MIB indicates that events of the same type, either up or down, must be able to be correlated into ranges. The implementation of these notifications does not do any of this correlation. A notification is generated for each individual VC that has an operational state change if that notification is enabled. A notification does not signal an operational state change for a group of VCs as described in the MIB.

## Benefits of the PWE3 MIBs

The PWE3 MIBs provide the ability to manage pseudowire emulation edge-to-edge by providing MPLS-related information about the service and a mechanism to monitor the Ethernet, Frame Relay, or ATM access circuits.

# How to Configure Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

This section contains the following procedures:

- [Enabling the SNMP Agent for the PWE3 MIBs, page 20](#) (required)
- [Configuring AToM, Frame Relay, or ATM Circuits Across a Network for the PWE3 MIBs, page 22](#) (required)

## Enabling the SNMP Agent for the PWE3 MIBs

Perform this task to enable the SNMP agent.

### SUMMARY STEPS

1. **enable**
2. **show running-config [interface | map-class]**

3. **configure terminal**
4. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6 nacl**] [*access-list-number*]
5. **end**
6. **write memory**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
	<b>Example:</b> Router> enable	
Step 2	<b>show running-config</b> [interface   map-class]	Displays the running configuration of the router so that you can determine if an SNMP agent is already running on the device.
	<b>Example:</b> Router# show running-config	<p>If no SNMP information is displayed, continue with the next step.</p> <p>If any SNMP information is displayed, you can modify the information or change it as desired.</p> <ul style="list-style-type: none"> <li>The optional <b>interface</b> keyword displays interface-specific configuration information.</li> <li>The optional <b>map-class</b> keyword displays dialer or Frame Relay map-class information.</li> </ul>
Step 3	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	

	Command or Action	Purpose
Step 4	<pre>snmp-server community <i>string</i> [<i>view view-name</i>] [<i>ro</i>   <i>rw</i>] [<i>ipv6 nacl</i>] [<i>access-list-number</i>]</pre> <p><b>Example:</b> Router(config)# snmp-server community public ro</p>	<p>Sets up the community access string to permit access to SNMP for the MIBs.</p> <ul style="list-style-type: none"> <li>The <i>string</i> argument consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string.</li> <li>The optional <b>view</b> <i>view-name</i> keyword argument combination specifies a previously defined view. The view defines the objects available to the SNMP community.</li> <li>The optional <b>ro</b> keyword configures read-only (ro) access to the objects in the MIBs.</li> <li>The optional <b>rw</b> keyword specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.</li> <li>The optional <b>ipv6</b> <i>nacl</i> keyword argument combination specifies an IPv6 named access list.</li> <li>The optional <i>access-list-number</i> argument is an integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent. Alternatively, it is an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.</li> </ul>
Step 5	<pre>end</pre> <p><b>Example:</b> Router(config)# end</p>	Exits to privileged EXEC mode.
Step 6	<pre>write memory</pre> <p><b>Example:</b> Router# write memory</p>	Writes the modified SNMP configuration into NVRAM of the router, permanently saving the SNMP settings.

## Configuring AToM, Frame Relay, or ATM Circuits Across a Network for the PWE3 MIBs

This section contains the following procedure:

- [Configuring the Pseudowire Class, page 23](#)

## Configuring the Pseudowire Class

The successful transmission of the Layer 2 frames between PE routers is due to the configuration of the PE routers. You configure the connection, called a pseudowire, between the routers.

**Note**

In simple configurations, this task is optional. You do not need to specify a pseudowire class if you specify the tunneling method as part of the **xconnect** command.

The pseudowire-class configuration group specifies the following characteristics of the tunneling mechanism:

- Encapsulation type
- Control protocol
- Payload-specific options

For more information, see the **pseudowire-class** command in the following feature module:

[Layer 2 Tunnel Protocol Version 3](#)

You must specify the **encapsulation mpls** command as part of the pseudowire class or as part of the **xconnect** command for the AToM VCs to work properly. If you omit the **encapsulation mpls** command as part of the **xconnect** command, you receive the following error:

```
% Incomplete command.
```

Once you specify the **encapsulation mpls** command, you cannot remove it using the **no encapsulation mpls** command. Nor can you change the command's setting using the **encapsulation l2tpv3** command. Those methods result in the following error message:

```
Encapsulation changes are not allowed on an existing pw-class.
```

To remove the command, you must delete the pseudowire with the **no pseudowire-class** command. To change the type of encapsulation, remove the pseudowire with the **no pseudowire-class** command and reestablish the pseudowire and specify the new encapsulation type.

**Note**

There are many options that you can configure. For detailed information, see the [Any Transport over MPLS](#) feature module.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **pseudowire-class** *name*
4. **encapsulation mpls**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>pseudowire-class name</code>  <b>Example:</b> <code>Router(config)# pseudowire-class atom</code>	Establishes a pseudowire class with a name that you specify and enters pseudowire class configuration mode.
Step 4	<code>encapsulation mpls</code>  <b>Example:</b> <code>Router(config-pw)# encapsulation mpls</code>	Specifies the tunneling encapsulation. For AToM, the encapsulation type is <b>mpls</b> .

## What to Do Next

Perform a MIB walk using your SNMP management tool on cpwVcMIB, cpwVcMplsMIB, cpwVcEnetMIB, cpwVcFrMIB, and cpwVcAtmMIB to verify that the PW-MIB, the PW-MPLS-MIB, the PW-ENET-MIB, the PW-FR-MIB, and the PW-ATM-MIB objects, respectively, are populated correctly.

**Note**

SNMPv1 and SNMPv2c are supported.

## Configuration Examples for the Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

This section provides the following configuration example:

- [PWE3 MIBs: Example, page 24](#)

### PWE3 MIBs: Example

In the following example, the configuration permits any SNMP manager to access all objects with read-only permissions using the community string *public*.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.  
Router(config)# **snmp-server community public ro**

**Note**

There is no explicit way to configure the PWE3 MIBs. However, for information on AToM configuration tasks and examples, see the [Any Transport over MPLS](#) feature module.

There are notifications specific to the PWE3 MIBs. For detailed information on the commands used to configure them, see the [“Additional References” section on page 25](#).

## Additional References

The following sections provide references related to the Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services feature.

## Related Documents

Related Topic	Document Title
SNMP commands	<a href="#">Cisco IOS Network Management Command Reference</a>
SNMP configuration tasks	<a href="#">Configuring SNMP Support</a>
Ethernet over MPLS configuration tasks	<a href="#">Any Transport over MPLS</a>
Frame Relay configuration tasks	<a href="#">Configuring Frame Relay</a>
ATM configuration tasks	<a href="#">Configuring ATM</a>
Pseudowire-related Internet drafts	<ul style="list-style-type: none"> <li>• <i>An Architecture for Multi-Segment Pseudo Wire Emulation Edge-to-Edge</i>, Internet draft, December 2007 [draft-ietf-pwe3-ms-arch-03.txt]</li> <li>• <i>Definitions for Textual Conventions and OBJECT-IDENTITIES for Pseudo-Wires Management</i>, Internet draft, August 10, 2007 [draft-ietf-pwe3-pw-tc-mib-09.txt]</li> <li>• <i>Ethernet Pseudo Wire (PW) Management Information Base</i>, Internet draft, August 30, 2007 [draft-pwe3-enet-mib-10.txt]</li> <li>• <i>Managed Objects for ATM over Packet Switched Network (PSN)</i>, Internet draft, August 8, 2007 [draft-ietf-pwe3-pw-atm-mib-02.txt]</li> <li>• <i>Pseudo Wire (PW) Management Information Base</i>, Internet draft, May 31, 2007 [draft-ietf-pwe3-pw-mib-11.txt]</li> <li>• <i>Pseudo Wire (PW) over MPLS PSN Management Information Base</i>, Internet draft, August 11, 2007 [draft-ietf-pwe3-pw-mpls-mib-11.txt]</li> </ul> <p><b>Note</b> For information on using SNMP MIB features, see the appropriate documentation for your network management system.</p>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
SNMP-VACM-MIB	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 1156	Management Information Base for Network Management of TCP/IP-based Internets
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
RFC 1315	Management Information Base for Frame Relay DTEs
RFC 3815	Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
RFC 3916	Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
RFC 4619	Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This feature uses no new or modified commands.



## Feature Information for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services

Table 14 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

---

Table 14 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

---

**Table 14**      **Feature Information for Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services**

Feature Name	Releases	Feature Information
Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services	12.0(29)S 12.0(30)S 12.0(31)S 12.2(28)SB 12.2(33)SRA 12.4(11)T 12.2(33)SXH	<p>The Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services feature provides Simple Network Management Protocol (SNMP) support within an Any Transport over Multiprotocol Label Switching (AToM) infrastructure emulating Ethernet, Frame Relay, and ATM services over packet switched networks (PSNs).</p> <p>In Cisco IOS Release 12.0(29)S, this feature was introduced as Pseudowire Emulation Edge-to-Edge MIBs for Ethernet Services.</p> <p>In Cisco IOS Release 12.0(30)S, the title changed to Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services because Frame Relay was added as a transport. Support was added for the Cisco 12000 series routers and for the CISCO-IETF-PW-FR-MIB (PW-FR-MIB).</p> <p>In Cisco IOS Release 12.0(31)S, the CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB) was modified regarding how cross-connect (XC) and tunnel indexes appear for virtual circuits (VCs).</p> <p>In Cisco IOS Release 12.2(28)SB, the title changed to Pseudowire Emulation Edge-to-Edge MIBs for Ethernet, Frame Relay, and ATM Services because ATM was added as a transport. Support was added for the CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB).</p> <p>In Cisco IOS Releases 12.2(33)SRA, 12.4(11)T, and 12.2(33)SXH, this feature was integrated into the releases as the Pseudowire Emulation Edge-to-Edge MIBs for Ethernet and Frame Relay Services feature because ATM is not supported as a transport.</p>

# Glossary

**AAL**—ATM adaptation layer. AAL defines the conversion of user information into cells. AAL1 and AAL2 handle isochronous traffic, such as voice and video; AAL3/4 and AAL5 pertain to data communications through the segmentation and reassembly of packets.

**ATM**—asynchronous transfer mode. A cell-based data transfer technique in which channel demand determines packet allocation. This is an international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media such as E3, SONET, and T3.

**CE router**—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router.

**DLCI**—data-link connection identifier. A unique number assigned to a PVC endpoint in a Frame Relay network. Identifies a particular PVC endpoint within an access channel in a Frame Relay network and has local significance only to that channel.

**encapsulation**—Wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging occurs in dissimilar networks, the entire frame from one network is simply placed in the header used by the data link layer protocol of the other network.

**EoMPLS**—ethernet over multiprotocol label switching (MPLS). A tunneling mechanism that allows a service provider to tunnel customer Layer 2 traffic through a Layer 3 MPLS network. EoMPLS is a point-to-point solution only. EoMPLS is also known as Layer 2 tunneling.

**Frame Relay**—The industry standard, switched data link layer protocol that handles multiple virtual circuits using High-Level Data Link Control (HDLC) encapsulation between connected devices. Frame Relay is more efficient than X.25, the protocol for which it is generally considered a replacement.

**IETF**—internet engineering task force. A task force (consisting of more than 80 working groups) that is developing standards for the Internet and the IP suite of protocols.

**LDP**—label distribution protocol. The protocol that supports MPLS hop-by-hop forwarding and the distribution of bindings between labels and network prefixes. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP**—label-switched path. A configured connection between two label switch routers (LSRs) in which label-switching techniques are used for packet forwarding; also a specific path through an MPLS network.

**LSR**—label switch router. A Multiprotocol Label Switching (MPLS) node that can forward native Layer 3 packets. The LSR forwards a packet based on the value of a label attached to the packet.

**MIB**—management information base. A database of network management information that is used and maintained by a network management protocol such as simple network management protocol (SNMP). The value of a MIB object can be changed or retrieved by using SNMP commands, usually through a network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—multiprotocol label switching. A switching method for the forwarding of IP traffic through the use of a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**MTU**—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can handle.

**NMS**—network management system. System responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. An NMS communicates with agents to help keep track of network statistics and resources.

**notification**—A message sent by a Simple Network Management Protocol (SNMP) agent to a network management station, console, or terminal to indicate that a significant network event has occurred. *See also* trap.

**OSPF**—Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**PE router**—provider edge router. A router that is part of a service provider's network and is connected to a customer edge (CE) router.

**primary tunnel**—A tunnel whose label-switched path (LSP) may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**pseudowire**—PW. A mechanism that carries the elements of an emulated service from one provider edge (PE) to one or more PEs over a packet switched network (PSN).

**SNMP**—simple network management protocol. A management protocol used almost exclusively in TCP/IP networks. SNMP provides a means for monitoring and controlling network devices, and for managing configurations, statistics collection, performance, and security.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal, indicating that a significant event occurred. Traps are less reliable than notification requests because the receiver does not send an acknowledgment when it receives a trap. The sender cannot determine if the trap was received.

**tunnel**—A secure communication path between two peers, such as routers.

**VC**—virtual circuit. A logical circuit created to ensure reliable communication between two network devices. A virtual circuit can be either permanent (PVC) or switched (SVC).

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLynX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

---

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

© 2007-2009 Cisco Systems, Inc. All rights reserved.





# MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

---

**First Published: January 26, 2004**

**Last Updated: February 27, 2009**

The MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature helps service providers monitor label switched paths (LSPs) and quickly isolate Multiprotocol Label Switching (MPLS) forwarding problems.

The feature provides the following capabilities:

- MPLS LSP ping to test LSP connectivity for IPv4 Label Distribution Protocol (LDP) prefixes, Resource Reservation Protocol (RSVP) traffic engineering (TE), and Any Transport over MPLS (AToM) forwarding equivalence classes (FECs).
- MPLS LSP traceroute to trace the LSPs for IPv4 LDP prefixes and RSVP TE prefixes.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV” section on page 60](#).

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

## Contents

- [Prerequisites for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 2](#)
- [Restrictions for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 2](#)



---

**Americas Headquarters:**

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

- [Information About MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 3](#)
- [How to Configure MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 10](#)
- [Configuration Examples for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 30](#)
- [Additional References, page 57](#)
- [Command Reference, page 59](#)
- [Feature Information for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV, page 60](#)
- [Glossary, page 62](#)

## Prerequisites for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

Before you use the MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature, you should:

- Determine the baseline behavior of your MPLS network. For example:
  - Expected MPLS experimental (EXP) treatment.
  - Expected maximum size packet or maximum transmission unit (MTU) of the LSP.
  - The topology, expected label switched path, and number of links in the LSP. Trace the paths of the label switched packets including the paths for load balancing.
- Understand how to use MPLS and MPLS applications. You need to:
  - Know how LDP is configured.
  - Understand AToM concepts.
- Understand label switching, forwarding, and load balancing.

Before using the **ping mpls** or **trace mpls** command, you must ensure that the router is configured to encode and decode MPLS echo packets in a format that all receiving routers in the network can understand.

## Restrictions for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

- You cannot use MPLS LSP traceroute to trace the path taken by AToM packets. MPLS LSP traceroute is not supported for AToM. (MPLS LSP ping is supported for AToM.) However, you can use MPLS LSP traceroute to troubleshoot the Interior Gateway Protocol (IGP) LSP that is used by AToM.
- You cannot use MPLS LSP ping to validate or trace MPLS Virtual Private Networks (VPNs).
- You cannot use MPLS LSP traceroute to troubleshoot LSPs that employ time-to-live (TTL) hiding.
- MPLS supports per-destination and per-packet (round robin) load balancing. If per-packet load balancing is in effect, you should not use MPLS LSP traceroute because LSP traceroute at a transit router consistency checks the information supplied in the previous echo response from the directly connected upstream router. When round robin is employed, the path that an echo request packet

takes cannot be controlled in a way that allows a packet to be directed to TTL expire at a given router. Without that ability, the consistency checking may fail during an LSP traceroute. A consistency check failure return code may be returned.

- A platform must support LSP ping and traceroute in order to respond to an MPLS echo request packet.
- Unless the MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature is enabled along the entire path, you cannot get a reply if the request fails along the path at any node.
- There are certain limitations when a mixture of draft versions are implemented within a network. The version of the draft must be compatible with Cisco's implementation. Due to the way the LSP Ping draft was written, earlier versions may not be compatible with later versions because of changes to type, length, values (TLVs) formats without sufficient versioning information. Cisco attempts to compensate for this in its implementations by allowing the sending and responding routers to be configured to encode and decode echo packets assuming a certain version.
- If you want to use MPLS LSP traceroute, the network should not use TTL hiding.

## Information About MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

Before using the MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature, you should understand the following concepts:

- [MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV Functionality, page 3](#)
- [MPLS LSP Ping Operation, page 4](#)
- [MPLS LSP Traceroute Operation, page 5](#)
- [MPLS Network Management with MPLS LSP Ping and MPLS LSP Traceroute, page 7](#)
- [Any Transport over MPLS Virtual Circuit Connection, page 7](#)
- [IP Does Not Forward MPLS Echo Request Packets, page 9](#)

## MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV Functionality

Internet Control Message Protocol (ICMP) ping and traceroute are often used to help diagnose the root cause when a forwarding failure occurs. However, they are not well suited for identifying LSP failures because an ICMP packet can be forwarded via IP to the destination when an LSP breakage occurs.

The MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature is well suited for identifying LSP breakages for the following reasons:

- An MPLS echo request packet cannot be forwarded via IP because IP TTL is set to 1 and the IP destination address field is set to a 127/8 address.
- The FEC being checked is not stored in the IP destination address field (as is the case of ICMP).

MPLS echo request and reply packets test LSPs. There are two methods by which a downstream router can receive packets:

- The Cisco implementation of MPLS echo request and echo reply that was previously based on the Internet Engineering Task Force (IETF) Internet Draft *Detecting MPLS Data Plane Failures* (draft-ietf-mpls-lsp-ping-03.txt).



- Features described in this document that are based on the IETF RFC 4379 *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*:
  - Echo request output interface control
  - Echo request traffic pacing
  - Echo request end-of-stack explicit-null label shimming
  - Echo request request-dsmap capability
  - Request-fec checking
  - Depth limit reporting

## MPLS LSP Ping Operation

MPLS LSP ping uses MPLS echo request and reply packets to validate an LSP. You can use MPLS LSP ping to validate IPv4 LDP, AToM, and IPv4 RSVP FECs by using appropriate keywords and arguments with the **ping mpls** command.

The MPLS echo request packet is sent to a target router through the use of the appropriate label stack associated with the LSP to be validated. Use of the label stack causes the packet to be forwarded over the LSP itself.

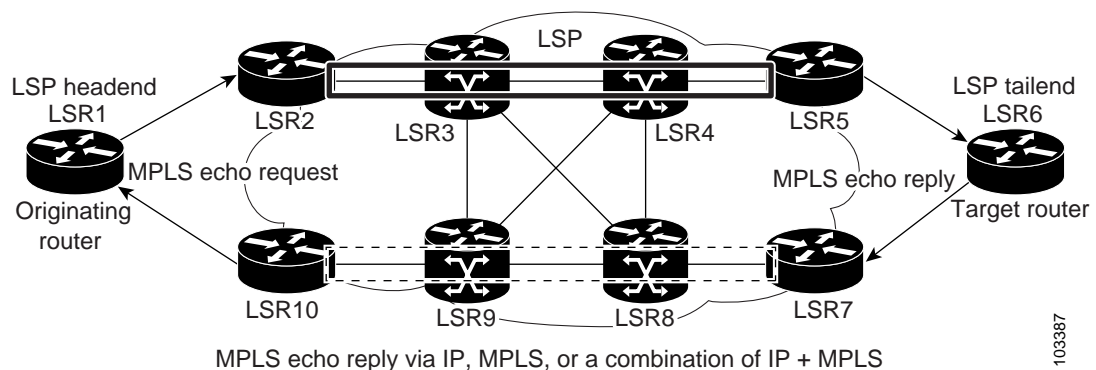
The destination IP address of the MPLS echo request packet is different from the address used to select the label stack. The destination IP address is defined as a 127.x.y.z/8 address. The 127.x.y.z/8 address prevents the IP packet from being IP switched to its destination if the LSP is broken.

An MPLS echo reply is sent in response to an MPLS echo request. The reply is sent as an IP packet and it is forwarded using IP, MPLS, or a combination of both types of switching. The source address of the MPLS echo reply packet is an address obtained from the router generating the echo reply. The destination address is the source address of the router that originated the MPLS echo request packet.

The MPLS echo reply destination port is set to the echo request source port.

Figure 1 shows MPLS LSP ping echo request and echo reply paths.

**Figure 1** MPLS LSP Ping Echo Request and Echo Reply Paths



If you initiate an MPLS LSP ping request at LSR1 to a FEC at LSR6, you get the results shown in Table 1.

**Table 1**      **MPLS LSP Ping Example from Figure 1**

Step	Router	Action
1.	LSR1	Initiates an MPLS LSP ping request for an FEC at the target router LSR6 and sends an MPLS echo request to LSR2.
2.	LSR2	Receives the MPLS echo request packet and forwards it through transit routers LSR3 and LSR4 to the penultimate router LSR5.
3.	LSR5	Receives the MPLS echo request, pops the MPLS label, and forwards the packet to LSR6 as an IP packet.
4.	LSR6	Receives the IP packet, processes the MPLS echo request, and sends an MPLS echo reply to LSR1 through an alternate route.
5.	LSR7 to LSR10	Receives the MPLS echo reply and forwards it back toward LSR1, the originating router.
6.	LSR1	Receives the MPLS echo reply in response to its MPLS echo request.

## MPLS LSP Traceroute Operation

MPLS LSP traceroute uses MPLS echo request and reply packets to validate an LSP. You can use MPLS LSP traceroute to validate IPv4 LDP and IPv4 RSVP FECs by using appropriate keywords and arguments with the **trace mpls** command.

The MPLS LSP Traceroute feature uses TTL settings to force expiration of the TTL along an LSP. MPLS LSP Traceroute incrementally increases the TTL value in its MPLS echo requests (TTL = 1, 2, 3, 4) to discover the downstream mapping of each successive hop. The success of the LSP traceroute depends on the transit router processing the MPLS echo request when it receives a labeled packet with a TTL = 1. On Cisco routers, when the TTL expires, the packet is sent to the Route Processor (RP) for processing. The transit router returns an MPLS echo reply containing information about the transit hop in response to the TTL-expired MPLS packet.

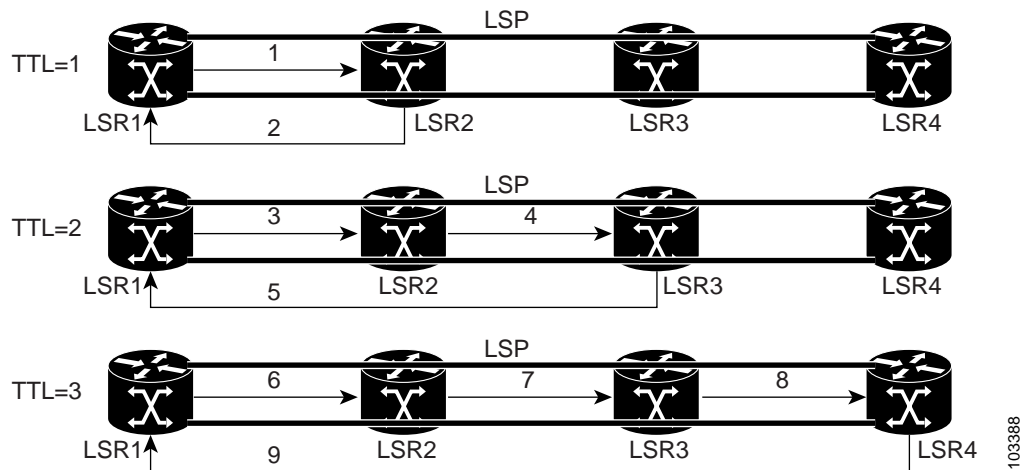
The MPLS echo reply destination port is set to the echo request source port.



### Note

When a router traces an IPV4 FEC that goes over a traffic engineering tunnel, intermediate routers may return U (unreachable) if LDP is not running in those intermediate routers.

Figure 2 shows an MPLS LSP traceroute example with an LSP from LSR1 to LSR4.

**Figure 2** *MPLS LSP Traceroute Example*

If you enter an LSP traceroute to an FEC at LSR4 from LSR1, you get the results shown in [Table 2](#).

**Table 2** *MPLS LSP Traceroute Example Based on [Figure 2](#)*

Step	Router	MPLS Packet Type and Description	Router Action (Receive or Send)
1.	LSR1	MPLS echo request—With a target FEC pointing to LSR4 and to a downstream mapping	<ul style="list-style-type: none"> <li>Sets the TTL of the label stack to 1</li> <li>Sends the request to LSR2</li> </ul>
2.	LSR2	MPLS echo reply	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 1</li> <li>Processes the User Datagram Protocol (UDP) packet as an MPLS echo request</li> <li>Finds a downstream mapping and replies to LSR1 with its own downstream mapping, based on the incoming label</li> </ul>
3.	LSR1	MPLS echo request—With the same target FEC and the downstream mapping received in the echo reply from LSR2	<ul style="list-style-type: none"> <li>Sets the TTL of the label stack to 2</li> <li>Sends the request to LSR2</li> </ul>
4.	LSR2	MPLS echo request	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 2</li> <li>Decrements the TTL</li> <li>Forwards the echo request to LSR3</li> </ul>
5.	LSR3	MPLS reply packet	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 1</li> <li>Processes the UDP packet as an MPLS echo request</li> <li>Finds a downstream mapping and replies to LSR1 with its own downstream mapping based on the incoming label</li> </ul>
6.	LSR1	MPLS echo request—With the same target FEC and the downstream mapping received in the echo reply from LSR3	<ul style="list-style-type: none"> <li>Sets the TTL of the packet to 3</li> <li>Sends the request to LSR2</li> </ul>

103388

**Table 2** *MPLS LSP Traceroute Example Based on Figure 2 (continued)*

Step	Router	MPLS Packet Type and Description	Router Action (Receive or Send)
7.	LSR2	MPLS echo request	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 3</li> <li>Decrements the TTL</li> <li>Forwards the echo request to LSR3</li> </ul>
8.	LSR3	MPLS echo request	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 2</li> <li>Decrements the TTL</li> <li>Forwards the echo request to LSR4</li> </ul>
9.	LSR4	MPLS echo reply	<ul style="list-style-type: none"> <li>Receives the packet with a TTL = 1</li> <li>Processes the UDP packet as an MPLS echo request</li> <li>Finds a downstream mapping and also finds that the router is the egress router for the target FEC</li> <li>Replies to LSR1</li> </ul>

## MPLS Network Management with MPLS LSP Ping and MPLS LSP Traceroute

To manage an MPLS network, you must have the ability to monitor LSPs and quickly isolate MPLS forwarding problems. You need ways to characterize the liveness of an LSP and reliably detect when an LSP fails to deliver user traffic.

You can use MPLS LSP ping to verify the LSP that is used to transport packets destined for IPv4 LDP prefixes, and AToM PW FECs. You can use MPLS LSP traceroute to trace LSPs that are used to carry packets destined for IPv4 LDP prefixes.

An MPLS echo request is sent through an LSP to validate it. A TTL expiration or LSP breakage causes the transit router to process the echo request before it gets to the intended destination. The router returns an MPLS echo reply that contains an explanatory reply code to the originator of the echo request.

The successful echo request is processed at the egress of the LSP. The echo reply is sent via an IP path, an MPLS path, or a combination of both back to the originator of the echo request.

## Any Transport over MPLS Virtual Circuit Connection

AToM Virtual Circuit Connection Verification (VCCV) allows you to send control packets inband of an AToM PW from the originating provider edge (PE) router. The transmission is intercepted at the destination PE router, instead of being forwarded to the customer edge (CE) router. This capability allows you to use MPLS LSP ping to test the PW section of AToM virtual circuits (VCs).

LSP ping allows verification of AToM VC setup by FEC 128 or FEC 129. FEC 128-based AToM VCs can be set up by using LDP for signaling or by using a static pseudowire configuration without using any signaling component on the two endpoints. Cisco IOS does not distinguish between FEC 128 and FEC 129 static pseudowires while issuing MPLS ping; the same commands are used.

AToM VCCV consists of the following:

- A signaled component in which the AToM VCCV capabilities are advertised during VC label signaling
- A switching component that causes the AToM VC payload to be treated as a control packet

## AToM VCCV Signaling

One of the steps involved in AToM VC setup is the signaling or communication of VC labels and AToM VCCV capabilities between AToM VC endpoints. To communicate the AToM VCCV disposition capabilities of each endpoint, the router uses an optional parameter, defined in the IETF Internet Draft *Pseudo Wire (PW) Virtual Circuit Connection Verification (VCCV)* (draft-ietf-pwe3-vccv-01).

The AToM VCCV disposition capabilities are categorized as follows:

- Applications—MPLS LSP ping and ICMP ping are applications that AToM VCCV supports to send packets inband of an AToM PW for control purposes.
- Switching modes—Type 1 and Type 2 are switching modes that AToM VCCV uses for differentiating between control and data traffic.

Table 3 describes AToM VCCV Type 1 and Type 2 switching modes.

**Table 3**      **Type 1 and Type 2 AToM VCCV Switching Modes**

Switching Mode	Description
Type 1	Uses a Protocol ID (PID) field in the AToM control word to identify an AToM VCCV packet
Type 2	Uses an MPLS Router Alert Label above the VC label to identify an AToM VCCV packet

## Selection of AToM VCCV Switching Types

Cisco routers always use Type 1 switching, if available, when they send MPLS LSP ping packets over an AToM VC control channel. Type 2 switching accommodates those VC types and implementations that do not support or interpret the AToM control word.

Table 4 shows the AToM VCCV switching mode advertised and the switching mode selected by the AToM VC.

**Table 4**      **AToM VCCV Switching Mode Advertised and Selected by AToM VC**

Type Advertised	Type Selected
AToM VCCV not supported	—
Type 1 AToM VCCV switching	Type 1 AToM VCCV switching
Type 2 AToM VCCV switching	Type 2 AToM VCCV switching
Type 1 and Type 2 AToM VCCV switching	Type 1 AToM VCCV switching

An AToM VC advertises its AToM VCCV disposition capabilities in both directions: that is, from the originating router (PE1) to the destination router (PE2), and from PE2 to PE1.

In some instances, AToM VCs might use different switching types if the two endpoints have different AToM VCCV capabilities. If PE1 supports Type 1 and Type 2 AToM VCCV switching and PE2 supports only Type 2 AToM VCCV switching, there are two consequences:

- LSP ping packets sent from PE1 to PE2 are encapsulated with Type 2 switching.
- LSP ping packets sent from PE2 to PE1 use Type 1 switching.

You can determine the AToM VCCV capabilities advertised to and received from the peer by entering the **show mpls l2transport binding** command at the PE router.

## Information Provided by the Router Processing LSP Ping or LSP Traceroute

Table 5 describes the characters that the router processing an LSP ping or LSP traceroute packet returns to the sender about the failure or success of the request.

You can also display the return code for an MPLS LSP Ping operation if you enter the **verbose** keyword in the **ping mpls** command.

**Table 5** *Echo Reply Return Codes*

Output Code	Echo Return Code	Meaning
x	0	No return code.
M	1	Malformed echo request.
m	2	Unsupported TLVs.
!	3	Success.
F	4	No FEC mapping.
D	5	DS Map mismatch.
I	6	Unknown Upstream Interface index.
U	7	Reserved.
L	8	Labeled output interface.
B	9	Unlabeled output interface.
f	10	FEC mismatch.
N	11	No label entry.
P	12	No receive interface label protocol.
p	13	Premature termination of the LSP.
X	unknown	Undefined return code.



**Note**

Echo return codes 6 and 7 are accepted only for Version 3 (draft-ietf-mpls-ping-03).

## IP Does Not Forward MPLS Echo Request Packets

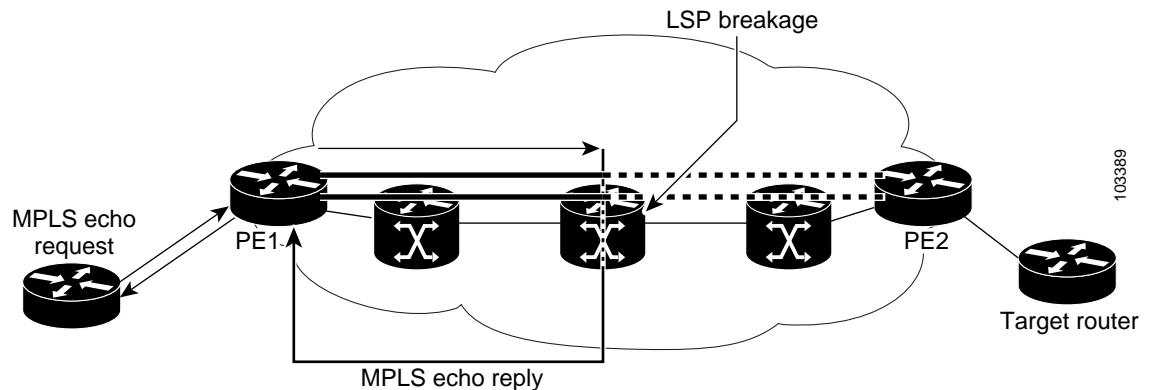
MPLS echo request packets sent during an LSP ping are never forwarded by IP. The IP header destination address field in an MPLS echo request packet is a 127.x.y.z/8 address. Routers should not forward packets using a 127.x.y.z/8 address. The 127.x.y.z/8 address corresponds to an address for the local host.

Use of a 127.x.y.z address as the destination address of the UDP packet is significant because the MPLS echo request packet fails to make it to the target router if a transit router does not label switch the LSP. The use of the 127.x.y.z address allows for the detection of LSP breakages. The following occurs at the transit router:

- If an LSP breakage occurs at a transit router, the MPLS echo packet is not forwarded; it is consumed by the router.
- If the LSP is intact, the MPLS echo packet reaches the target router and is processed by the terminal point of the LSP.

Figure 3 shows the path of the MPLS echo request and reply when a transit router fails to label switch a packet in an LSP.

**Figure 3** Path when Transit Router Fails to Label Switch a Packet



**Note**

An AToM payload does not contain usable forwarding information at a transit router because the payload may not be an IP packet. An MPLS VPN packet, although an IP packet, does not contain usable forwarding information at a transit router because the destination IP address is significant only to the virtual routing and forwarding (VRF) instances at the endpoints of the MPLS network.

## How to Configure MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

This section contains the following tasks:

- [Enabling Compatibility Between the MPLS LSP and Ping or Traceroute Implementation, page 11](#) (required)
- [Validating an FEC by Using MPLS LSP Ping and MPLS LSP Traceroute, page 12](#) (required)
- [Using DSCP to Request a Specific Class of Service in an Echo Reply, page 14](#) (optional)
- [Controlling How a Responding Router Replies to an MPLS Echo Request, page 15](#) (optional)
- [Preventing Loops when Using MPLS LSP Ping and LSP Traceroute Command Options, page 17](#) (optional)
- [Detecting LSP Breaks, page 19](#) (optional)

## Enabling Compatibility Between the MPLS LSP and Ping or Traceroute Implementation

LSP ping drafts after Version 3 (draft-ietf-mpls-ping-03) have undergone numerous TLV format changes, but the versions of the draft do not always interoperate.

To allow later Cisco implementations to interoperate with draft Version 3 Cisco and non-Cisco implementations, use a global configuration mode to decode echo packets in formats understood by draft Version 3 implementations.

Unless configured otherwise, a Cisco implementation encodes and decodes echo requests assuming the version on which the IETF implementations is based.

To prevent failures reported by the replying router due to TLV version issues, you should configure all routers in the core. Encode and decode MPLS echo packets in the same draft version. For example, if the network is running RFC 4379 (Cisco Version 4) implementations but one router is capable of only Version 3 (Cisco Revision 3), configure all routers in the network to operate in Revision 3 mode.

The Cisco implementation of MPLS echo request and echo reply is based on the IETF RFC 4379. IETF drafts subsequent to this RFC (drafts 3, 4, 5, 6, and 7) introduced TLV format differences. These differences could not be identified because the echo packet had no way to differentiate between one TLV format and another TLV format. This introduced limited compatibility between the MPLS LSP Ping/Traceroute implementations in the Cisco IOS 12.0(27)S1 and 12.0(27)S2 releases and the MPLS ping or traceroute implementation in later Cisco IOS releases. To allow interoperability between these releases, a **revision** keyword was added for the **ping mpls** and **trace mpls** commands. The **revision** keyword enables Cisco IOS releases to support the existing draft changes and any changes from future versions of the IETF LSP Ping draft.

**Note**

We recommend that you use the **mpls oam** global configuration command instead of the revision option.

**Note**

No images are available on cisco.com to support Revision 2. It is recommended that you use only images supporting Version 3 and later when configuring TLV encode and decode modes. MPLS Multipath LSP traceroute requires Cisco Revision 4 or later.

### Cisco Vendor Extensions

In Cisco's Version 3 (draft-ietf-mpls-ping-03.txt) implementations, Cisco defined a vendor extension TLV in the ignore-if-not-understood TLV space. It is used for the following purposes:

- Provide an ability to track TLV versions.
- Provide an experimental Reply TOS capability.

The first capability was defined before the existence of the global configuration command for setting the echo packet encode and decode behavior. TLV version information in an echo packet overrides the configured decoding behavior. Using this TLV for TLV versions is no longer required since the introduction of the global configuration capability.

The second capability controls the reply DSCP. Draft Version 8 defines a Reply TOS TLV, so the use of the reply DSCP is no longer required.

To enable compatibility between the MPLS LSP and ping or traceroute implementation by customizing the default behavior of echo packets, perform the following steps.



## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls oam**
4. **echo revision {3 | 4}**
5. **echo vendor-extension**
6. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>mpls oam</b>  <b>Example:</b> Router(config)# mpls oam	Enters MPLS OAM configuration mode for customizing the default behavior of echo packets.
Step 4	<b>echo revision {3   4}</b>  <b>Example:</b> Router(config-mpls)# echo revision 4	Specifies the revision number of the echo packet's default values. <ul style="list-style-type: none"><li>3—draft-ietf-mpls-ping-03 (Revision 2).</li><li>4—RFC 4379 compliant (default).</li></ul>
Step 5	<b>echo vendor-extension</b>  <b>Example:</b> Router(config-mpls)# echo vendor-extension	Sends the Cisco-specific extension of TLVs with echo packets.
Step 6	<b>exit</b>  <b>Example:</b> Router(config-mpls)# exit	Returns to global configuration mode.

## Validating an FEC by Using MPLS LSP Ping and MPLS LSP Traceroute

An LSP is formed by labels. Routers learn labels through LDP, AToM, or some other MPLS applications. You can use MPLS LSP ping or traceroute to validate an LSP used for forwarding traffic for a given FEC.

This section describes the following tasks:

- [Validating an LDP IPv4 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute, page 13](#)

- [Validating a Layer 2 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute, page 14](#)

## Validating an LDP IPv4 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute

To ensure that the router will be able to forward MPLS packets for IPv4 FEC prefixes advertised by LDP, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **ping mpls ipv4** *destination-address/destination-mask-length* [**repeat** *count*] [**exp** *exp-bits*] [**verbose**]  
or  
**trace mpls ipv4** *destination-address/destination-mask-length*
3. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls ipv4</b> <i>destination-address/destination-mask-length</i> [ <b>repeat</b> <i>count</i> ] [ <b>exp</b> <i>exp-bits</i> ] [ <b>verbose</b> ]  or  <b>trace mpls ipv4</b> <i>destination-address/destination-mask-length</i>  <b>Example:</b> Router# ping mpls ipv4 10.131.191.252/32 exp 5 repeat 5 verbose  or  <b>Example:</b> Router# trace mpls ipv4 10.131.191.252/32	Selects an LDP IPv4 prefix FEC for validation.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Validating a Layer 2 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute

To ensure that the router will be able to forward MPLS packets for Layer 2 FEC prefixes advertised by LDP, perform the following steps.

### SUMMARY STEPS

- `enable`
- `ping mpls pseudowire ipv4-address vc-id vc-id`
- `exit`

### DETAILED STEPS

Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>ping mpls pseudowire ipv4-address vc-id vc-id</code>  <b>Example:</b> Router# <code>ping mpls pseudowire 10.131.191.252 vc-id 333</code>	Selects a Layer 2 FEC for validation.
Step 3	<code>exit</code>  <b>Example:</b> Router# <code>exit</code>	Returns to user EXEC mode.

## Using DSCP to Request a Specific Class of Service in an Echo Reply

For Cisco IOS Release 12.2(27)SXE, Cisco added a reply differentiated services code point (DSCP) option that lets you request a specific class of service (CoS) in an echo reply.

The reply DSCP option is supported in the experimental mode for IETF draft-ietf-mpls-lsp-ping-03.txt. Cisco implemented a vendor-specific extension for the reply DSCP option rather than using a Reply TOS TLV. A Reply TOS TLV serves the same purpose as the **reply dscp** command in RFC 4379. This draft provides a standardized method of controlling the reply DSCP.



#### Note

Before draft Version 8, Cisco implemented the Reply DSCP option as an experimental capability using a Cisco vendor extension TLV. If a router is configured to encode MPLS echo packets for draft Version 3 implementations, a Cisco vendor extension TLV is used instead of the Reply TOS TLV that was defined in draft Version 8.

To use DSCP to request a specific CoS in an echo reply, perform the following steps.

### SUMMARY STEPS

- `enable`

2. **ping mpls** {**ipv4** *destination-address/destination-mask-length* | **pseudowire** *ipv4-address vc-id vc-id* } [**reply dscp** *dscp-value*]  
or  
**trace mpls ipv4** *destination-address/destination-mask-length* [**reply dscp** *dscp-value*]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4</b> <i>destination-address/destination-mask-length</i>   <b>pseudowire</b> <i>ipv4-address vc-id vc-id</i> } [ <b>reply dscp</b> <i>dscp-value</i> ]  or <b>trace mpls ipv4</b> <i>destination-address/destination-mask-length</i> [ <b>reply dscp</b> <i>dscp-value</i> ]  <b>Example:</b> Router# ping mpls ipv4 10.131.191.252/32 reply dscp 50  or <b>Example:</b> Router# trace mpls ipv4 10.131.191.252/32 reply dscp 50	Controls the DSCP value of an echo reply.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Controlling How a Responding Router Replies to an MPLS Echo Request

To control how a responding router replies to an MPLS echo request, see the [“Reply Modes for an MPLS LSP Ping and LSP Traceroute Echo Request Response”](#) section.

### Reply Modes for an MPLS LSP Ping and LSP Traceroute Echo Request Response

The reply mode controls how a responding router replies to an MPLS echo request sent by a **ping mpls** or **trace mpls** command. There are two reply modes for an echo request packet:

- ipv4—Reply with an IPv4 UDP packet (default)

- router-alert—Reply with an IPv4 UDP packet with router alert

**Note**

It is useful to use `ipv4` and `router-alert` reply modes in conjunction with each other to prevent false negatives. If you do not receive a reply via the `ipv4` mode, it is useful to send a test with the `router-alert` reply mode. If both fail, something is wrong in the return path. The problem may be only that the Reply TOS is not set correctly.

**ipv4 Reply Mode**

IPv4 packet is the most common reply mode used with a **ping mpls** or **trace mpls** command when you want to periodically poll the integrity of an LSP. With this option, you do not have explicit control over whether the packet traverses IP or MPLS hops to reach the originator of the MPLS echo request. If the originating (headend) router fails to receive a reply to an MPLS echo request when you use the **reply mode ipv4** keywords, use the **reply mode router-alert** keywords.

**Router-alert Reply Mode**

The router-alert reply mode adds the router alert option to the IP header. When an IP packet that contains an IP router alert option in its IP header or an MPLS packet with a router alert label as its outermost label arrives at a router, the router punts (redirects) the packet to the Route Processor (RP) level for handling. This forces the Cisco router to handle the packet at each intermediate hop as it moves back to the destination. Hardware and line-card forwarding inconsistencies are bypassed. Router-alert reply mode is more expensive than IPv4 mode because the reply goes hop-by-hop. It also is slower, so the sender receives a reply in a relatively longer period of time.

Table 6 describes how IP and MPLS packets with an IP router alert option are handled by the router switching path processes.

**Table 6** Path Process Handling of IP and MPLS Router Alert Packets

Incoming Packet	Normal Switching Action	Process Switching Action	Outgoing Packet
IP packet—Router alert option in IP header	Router alert option in IP header causes the packet to be punted to the process switching path.	Forwards the packet as is	IP packet—Router alert option in IP header
		Forwards the packet as is	MPLS packet
MPLS packet—Outermost label contains a router alert	If the router alert label is the outermost label, it causes the packet to be punted to the process switching path.	Removes the outermost router alert label and forwards the packet as an IP packet	IP packet—Router alert option in IP header
		Preserves the outermost router alert label and forwards the MPLS packet	MPLS packet—Outermost label contains a router alert.

**SUMMARY STEPS**

1. **enable**
  2. **ping mpls** {**ipv4** *destination-address/destination-mask-length* | **pseudowire** *ipv4-address vc-id vc-id*} **reply mode** {**ipv4** | **router-alert**}
- or

```
trace mpls ipv4 destination-address/destination-mask reply mode {ipv4 | router-alert}
```

### 3. exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<pre>ping mpls {ipv4 destination-address /destination-mask-length   pseudowire ipv4-address vc-id vc-id} reply mode {ipv4   router-alert}</pre> <p>or</p> <pre>trace mpls ipv4 destination-address /destination-mask reply mode {ipv4   router-alert}</pre> <p><b>Example:</b> Router# ping mpls ipv4 10.131.191.252/32 reply mode ipv4</p> <p>or</p> <pre>Router# trace mpls ipv4 10.131.191.252/32 reply mode router-alert</pre>	Checks MPLS LSP connectivity. or Discovers MPLS LSP routes that packets actually take when traveling to their destinations.  <b>Note</b> To specify the reply mode, you must enter the <b>reply mode</b> keyword with the <b>ipv4</b> or <b>router-alert</b> keyword.
Step 3	<pre>exit</pre> <p><b>Example:</b> Router# exit</p>	Returns to user EXEC mode.

## Preventing Loops when Using MPLS LSP Ping and LSP Traceroute Command Options

The interaction of the MPLS Embedded Management—LSP Ping for LDP feature options can cause loops. See the following sections for a description of the loops you may encounter with the **ping mpls** and **trace mpls** commands:

- [Using MPLS LSP Ping to Discover Possible Loops, page 17](#)
- [Using MPLS LSP Traceroute to Discover Possible Loops, page 18](#)

## Using MPLS LSP Ping to Discover Possible Loops

With the MPLS LSP Ping feature, loops can occur if you use the UDP destination address range, repeat option, or sweep option.

To use MPLS LSP ping to discover possible loops, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **ping mpls** {**ipv4** *destination-address/destination-mask* [**destination** *address-start address-end increment*] | [**pseudowire** *ipv4-address vc-id vc-id address-end increment*] } [**repeat** *count*] [**sweep** *minimum maximum size-increment*]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4</b> <i>destination-address /destination-mask</i> [ <b>destination</b> <i>address-start address-end increment</i> ]   [ <b>pseudowire</b> <i>ipv4-address vc-id vc-id address-end increment</i> ]} [ <b>repeat</b> <i>count</i> ] [ <b>sweep</b> <i>minimum maximum size-increment</i> ]  <b>Example:</b> Router# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 1 repeat 2 sweep 1450 1475 25	Checks MPLS LSP connectivity.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Using MPLS LSP Traceroute to Discover Possible Loops

With the MPLS LSP Traceroute feature, loops can occur if you use the UDP destination address range option and the time-to-live option.

By default, the maximum TTL is set to 30. Therefore, the traceroute output may contain 30 lines if the target of the traceroute is not reached, which can happen when an LSP problem exists. If an LSP problem occurs, there may be duplicate entries. The router address of the last point that the trace reaches is repeated until the output is 30 lines. You can ignore the duplicate entries.

## SUMMARY STEPS

1. **enable**
2. **trace mpls ipv4** *destination-address/destination-mask* [**destination** *address-start address-end address-increment*] [**ttl** *maximum-time-to-live*]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>trace mpls ipv4 destination-address /destination-mask [destination address-start address-end address increment] [ttl maximum-time-to-live]</b>  <b>Example:</b> Router# trace mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.3 1 ttl 5	Discovers MPLS LSP routes that packets take when traveling to their destinations. The example shows how a loop can occur.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Detecting LSP Breaks

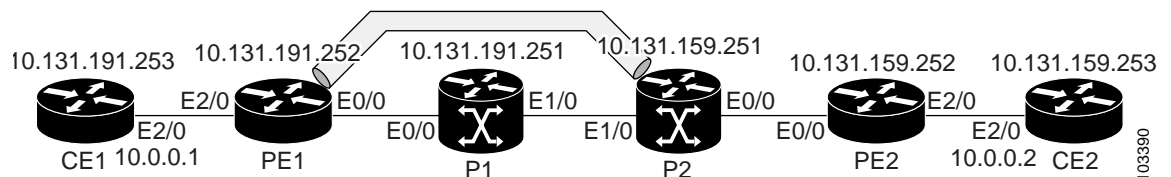
If there is a problem forwarding MPLS packets in your network, you can determine where there are LSP breaks. This section describes MTU discovery in an LSP.

Untagged output interfaces at a penultimate hop do not impact the forwarding of IP packets through an LSP because the forwarding decision is made at the penultimate hop through use of the incoming label. However, untagged output interfaces cause AToM and MPLS VPN traffic to be dropped at the penultimate hop.

During an MPLS LSP ping, MPLS echo request packets are sent with the IP packet attribute set to “do not fragment.” That is, the Don’t Fragment (DF) bit is set in the IP header of the packet. This allows you to use the MPLS echo request to test for the MTU that can be supported for the packet through the LSP without fragmentation.

Figure 4 shows a sample network with a single LSP from PE1 to PE2 formed with labels advertised by the LDP.

**Figure 4** Sample Network with LSP—Labels Advertised by LDP





You can determine the maximum receive unit (MRU) at each hop by using the MPLS Traceroute feature to trace the LSP. The MRU is the maximum size of a labeled packet that can be forwarded through an LSP.

This section contains the following tasks:

- [Tracking Packets Tagged as Implicit Null, page 20](#)
- [Tracking Untagged Packets, page 21](#)
- [Determining Why a Packet Could Not Be Sent, page 21](#)
- [Detecting LSP Breaks when Load Balancing Is Enabled for IPv4 LDP LSPs, page 22](#)
- [Specifying the Interface Through Which Echo Packets Leave a Router, page 23](#)
- [Pacing the Transmission of Packets, page 24](#)
- [Interrogating the Transit Router for Its Downstream Information by Using Echo Request request-dsmap, page 25](#)
- [Interrogating a Router for Its DSMAP, page 26](#)
- [Requesting that a Transit Router Validate the Target FEC Stack, page 27](#)
- [Enabling LSP Ping to Detect LSP Breakages Caused by Untagged Interfaces, page 28](#)
- [Viewing the AToM VCCV Capabilities Advertised to and Received from the Peer, page 29](#)

## Tracking Packets Tagged as Implicit Null

To track packets tagged as implicit null, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **trace mpls ipv4** *destination-address* /*destination-mask*
3. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>trace mpls ipv4</b> <i>destination-address</i> / <i>destination-mask</i>  <b>Example:</b> Router# trace mpls ipv4 10.131.159.252/32	Discovers MPLS LSP routes that packets actually take when traveling to their destinations.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Tracking Untagged Packets

To track untagged packets, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show mpls forwarding-table** *destination-address/destination-mask*
3. **show mpls ldp discovery**
4. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show mpls forwarding-table</b> <i>destination-address/destination-mask</i>  <b>Example:</b> Router# show mpls forwarding-table 10.131.159.252/32	Displays the content of the MPLS Label Forwarding Information Base (LFIB) and displays whether the LDP is properly configured.
Step 3	<b>show mpls ldp discovery</b>  <b>Example:</b> Router# show mpls ldp discovery	Displays the status of the LDP discovery process and displays whether the LDP is properly configured.
Step 4	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Determining Why a Packet Could Not Be Sent

The Q return code means that the packet could not be sent. The problem can be caused by insufficient processing memory, but it probably results because an LSP could not be found that matches the FEC information that was entered on the command line.

You need to determine the reason why the packet was not forwarded so that you can fix the problem in the path of the LSP. To do so, look at the Routing Information Base (RIB), the Forwarding Information Base (FIB), the Label Information Base (LIB), and the MPLS LFIB. If there is no entry for the FEC in any of these routing or forwarding bases, there is a Q return code.

To determine why a packet could not be transmitted, perform the following steps.

### SUMMARY STEPS

1. **enable**

2. **show ip route** [*ip-address* [**mask**]]
3. **show mpls forwarding-table** [*network* {*mask* | *length*} | **labels** *label* [- *label*] | **interface** *interface* | **next-hop** *address* | **lsp-tunnel** [*tunnel-id*]]
4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show ip route</b> [ <i>ip-address</i> [ <b>mask</b> ]]  <b>Example:</b> Router# show ip route 10.0.0.1	Displays the current state of the routing table.  When the MPLS echo reply returns a Q, troubleshooting occurs on the routing information database.
Step 3	<b>show mpls forwarding-table</b> [ <i>network</i> { <i>mask</i>   <i>length</i> }   <b>labels</b> <i>label</i> [- <i>label</i> ]   <b>interface</b> <i>interface</i>   <b>next-hop</b> <i>address</i>   <b>lsp-tunnel</b> [ <i>tunnel-id</i> ]]  <b>Example:</b> Router# show mpls forwarding-table 10.0.0.1/32	Displays the content of the MPLS LFIB. When the MPLS echo reply returns a Q, troubleshooting occurs on a label information database and an MPLS forwarding information database.
Step 4	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Detecting LSP Breaks when Load Balancing Is Enabled for IPv4 LDP LSPs

An ICMP ping or trace follows one path from the originating router to the target router. Round robin load balancing of IP packets from a source router discovers the various output paths to the target IP address.

For MPLS ping and traceroute, Cisco routers use the source and destination addresses in the IP header for load balancing when multiple paths exist through the network to a target router. The Cisco implementation of MPLS may check the destination address of an IP payload to accomplish load balancing (the type of checking depends on the platform).

To detect LSP breaks when load balancing is enabled for IPv4 LDP LSPs, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **ping mpls ipv4** *destination-address/destination-mask-length* [**destination** *address-start* *address-end* *increment*]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls ipv4 destination-address /destination-mask-length [destination address-start address-end increment]</b>  <b>Example:</b> Router# <b>ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1/8</b>	Checks for load balancing paths.  Enter the 127.z.y.x/8 destination address.
Step 3	<b>exit</b>  <b>Example:</b> Router# <b>exit</b>	Returns to user EXEC mode.

## Specifying the Interface Through Which Echo Packets Leave a Router

To specify the interface through which echo packets leave a router, perform the following steps.

### Echo Request Output Interface Control

You can control the interface through which packets leave a router. Path output information is used as input to LSP ping and traceroute.

The echo request output interface control feature allows you to force echo packets through the paths that perform detailed debugging or characterizing of the LSP. This feature is useful if a PE router connects to an MPLS cloud and there are broken links. You can direct traffic through a certain link. The feature also is helpful for troubleshooting network problems.

To specify the output interface for echo requests, perform the following steps.

## SUMMARY STEPS

- enable**
- ping mpls {ipv4 destination-address/destination-mask | pseudowire ipv4-address vc-id vc-id} [output interface tx-interface]**  
or  
**trace mpls ipv4 destination-address/destination-mask [output interface tx-interface]**
- exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4</b> <i>destination-address</i> / <i>destination-mask</i>   <b>pseudowire</b> <i>ipv4-address</i> <b>vc-id</b> <i>vc-id</i> } [ <b>output interface</b> <i>tx-interface</i> ]  or  <b>trace mpls ipv4</b> <i>destination-address/destination-mask</i> [ <b>output interface</b> <i>tx-interface</i> ]  <b>Example:</b> Router# ping mpls ipv4 10.131.159.251/32 output interface ethernet0/0  or  Router# trace mpls ipv4 10.131.159.251/32 output interface ethernet0/0	Checks MPLS LSP connectivity.  or  Discovers MPLS LSP routes that packets actually take when traveling to their destinations.  <b>Note</b> For this task, you must specify the <b>output interface</b> keyword.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Pacing the Transmission of Packets

Echo request traffic pacing allows you to pace the transmission of packets so that the receiving router does not drop packets. To perform echo request traffic pacing, perform the following steps.

## SUMMARY STEPS

- enable**
- ping mpls** {**ipv4** *destination-address/destination-mask* | **pseudowire** *ipv4-address* **vc-id** *vc-id*} [**interval** *ms*]  
  
or  
  
**trace mpls ipv4** *destination-address/destination-mask*
- exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4 destination-address</b> / <b>destination-mask</b>   <b>pseudowire ipv4-address vc-id vc-id</b> } [ <b>interval ms</b> ]  or  <b>trace mpls ipv4 destination-address</b> / <b>destination-mask</b>  <b>Example:</b> Router# ping mpls ipv4 10.131.159.251/32 interval 2  or  <b>Example:</b> Router# trace mpls ipv4 10.131.159.251/32	Checks MPLS LSP connectivity.  or  Discovers MPLS LSP routes that packets take when traveling to their destinations.  <b>Note</b> In this task, if you use the <b>ping mpls</b> command you must specify the <b>interval</b> keyword.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Interrogating the Transit Router for Its Downstream Information by Using Echo Request request-dsmap

The echo request request-dsmap capability troubleshooting feature, used in conjunction with the TTL flag, allows you to selectively interrogate a transit router. If there is a failure, you do not have to enter an **lsp traceroute** command for each previous failure; you can focus just on the failed hop.

A request-dsmap flag in the downstream mapping flags field, and procedures that specify how to trace noncompliant routers allow you to arbitrarily time-to-live (TTL) expire MPLS echo request packets with a wildcard downstream map (DSMAP).

Echo request DSMAPs received without labels indicate that the sender did not have any DSMAPs to validate. If the downstream router ID field of the DSMAP TLV in an echo request is set to the ALLROUTERS address (224.0.0.2) and there are no labels, the source router can arbitrarily query a transit router for its DSMAP information.

The **ping mpls** command allows an MPLS echo request to be TTL-expired at a transit router with a wildcard DSMAP for the explicit purpose of troubleshooting and querying the downstream router for its DSMAPs. The default is that the DSMAP has an IPv4 bitmap hashkey. You also can select hashkey 0 (none). The purpose of the **ping mpls** command is to allow the source router to selectively TTL expire an echo request at a transit router to interrogate the transit router for its downstream information. The ability to also select a multipath (hashkey) type allows the transmitting router to interrogate a transit router for load-balancing information as is done with multipath LSP traceroute, but without having to

interrogate all subsequent nodes traversed between the source router and the router on which each echo request TTL expires. Use an echo request in conjunction with the TTL setting because if an echo request arrives at the egress of the LSP with an echo request, the responding routers never return DSMAPs.

To interrogate the transit router for its downstream information so that you can focus just on the failed hop if there is a failure, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **ping mpls** {**ipv4** *destination-address/destination-mask* | **pseudowire** *ipv4-address vc-id vc-id*} [**dsmap** [**hashkey** {**none** | **ipv4** *bitmap bitmap-size*}]]
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4</b> <i>destination-address /destination-mask</i>   <b>pseudowire</b> <i>ipv4-address vc-id vc-id</i> } [ <b>dsmap</b> [ <b>hashkey</b> { <b>none</b>   <b>ipv4</b> <i>bitmap bitmap-size</i> }]]  <b>Example:</b> Router# ping mpls ipv4 10.161.251/32 dsmap hashkey ipv4 bitmap 16	Checks MPLS LSP connectivity.  <b>Note</b> In this task, you must specify the <b>dsmap</b> and <b>hashkey</b> keywords.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Interrogating a Router for Its DSMAP

The router can interrogate the software or hardware forwarding layer for the depth limit that needs to be returned in the DSMAP TLV. If forwarding does not provide a value, the default is 255.

To determine the depth limit, specify the **dsmap** and **ttl** keywords in the **ping mpls** command. The transit router will be interrogated for its DSMAP. The depth limit is returned with the echo reply DSMAP. A value of 0 means that the IP header is used for load balancing. Another value indicates that the IP header load balances up to the specified number of labels.

To interrogate a router for its DSMAP, perform the following steps.

## SUMMARY STEPS

1. **enable**

2. **ping mpls** {**ipv4** *destination-address/destination-mask* | **pseudowire** *ipv4-address vc-id vc-id*} **ttl** *time-to-live* **dsmap**
3. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls</b> { <b>ipv4</b> <i>destination-address /destination-mask</i>   <b>pseudowire</b> <i>ipv4-address vc-id vc-id</i> } <b>ttl</b> <i>time-to-live</i> <b>dsmap</b>  <b>Example:</b> Router# ping mpls ipv4 10.131.159.252/32 ttl 1 dsmap	Checks MPLS LSP connectivity.  <b>Note</b> You must specify the <b>ttl</b> and <b>dsmap</b> keywords.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Requesting that a Transit Router Validate the Target FEC Stack

An MPLS echo request tests a particular LSP. The LSP to be tested is identified by the FEC stack.

To request that a transit router validate the target FEC stack, set the V flag from the source router by entering the **flags fec** keyword in the **ping mpls** and **trace mpls** commands. The default is that echo request packets are sent with the V flag set to 0.

To request that a transit router validate the target FEC stack, perform the following steps.

## SUMMARY STEPS

1. **enable**
2. **ping mpls** {**ipv4** *destination-address/destination-mask* | **pseudowire** *ipv4-address vc-id vc-id*} **flags fec**  
or  
**trace mpls** **ipv4** *destination-address/destination-mask* **flags fec**
3. **exit**



## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>ping mpls {ipv4 destination-address /destination-mask   pseudowire ipv4-address vc-id vc-id} flags fec</b>  or  <b>trace mpls ipv4 destination-address /destination-mask flags fec</b>  <b>Example:</b> Router# ping mpls ipv4 10.131.159.252/32 flags fec  or  <b>Example:</b> Router# trace mpls ipv4 10.131.159.252/32 flags fec	Checks MPLS LSP connectivity.  or  Discovers MPLS LSP routes that packets actually take when traveling to their destinations.  <b>Note</b> You must enter the <b>flags fec</b> keyword.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Enabling LSP Ping to Detect LSP Breakages Caused by Untagged Interfaces

For MPLS LSP ping and traceroute of LSPs carrying IPv4 FECs, you can force an explicit null label to be added to the MPLS label stack even though the label was unsolicited. This allows LSP ping to detect LSP breakages caused by untagged interfaces. LSP ping does not report that an LSP is operational when it is unable to send MPLS traffic.

An explicit null label is added to an MPLS label stack if MPLS echo request packets are forwarded from untagged interfaces that are directly connected to the destination of the LSP ping or if the IP TTL value for the MPLS echo request packets is set to 1.

When you enter an **lsp ping** command, you are testing the LSP's ability to carry IP traffic. Failure at untagged output interfaces at the penultimate hop are not detected. Explicit-null shimming allows you to test an LSP's ability to carry MPLS traffic.

To enable LSP ping to detect LSP breakages caused by untagged interfaces, specify the **force-explicit-null** keyword in the **ping mpls** or **trace mpls** commands as shown in the following steps.

## SUMMARY STEPS

1. **enable**

2. **ping mpls {ipv4 destination-address/destination-mask | pseudowire ipv4-address vc-id vc-id} force-explicit-null**  
or  
**trace mpls ipv4 destination-address/destination-mask force-explicit-null**
3. **exit**

## DETAILED STEP

<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>ping mpls {ipv4 destination-address /destination-mask   pseudowire ipv4-address vc-id vc-id} force-explicit-null</b>  or <b>trace mpls ipv4 destination-address /destination-mask force-explicit-null</b>  <b>Example:</b> Router# ping mpls ipv4 10.131.191.252/32 force-explicit null  or  <b>Example:</b> Router# trace mpls ipv4 10.131.191.252/32 force-explicit-null	Checks MPLS LSP connectivity.  or Discovers MPLS LSP routes that packets actually take when traveling to their destinations.  <b>Note</b> You must enter the <b>force-explicit-null</b> keyword.
<b>Step 3</b>	<b>exit</b>  <b>Example:</b> Router# exit	Returns to user EXEC mode.

## Viewing the AToM VCCV Capabilities Advertised to and Received from the Peer

To view the AToM VCCV capabilities advertised to and received from the peer, perform the following steps.

### SUMMARY STEPS

1. **enable**
2. **show mpls l2transport binding**
3. **exit**

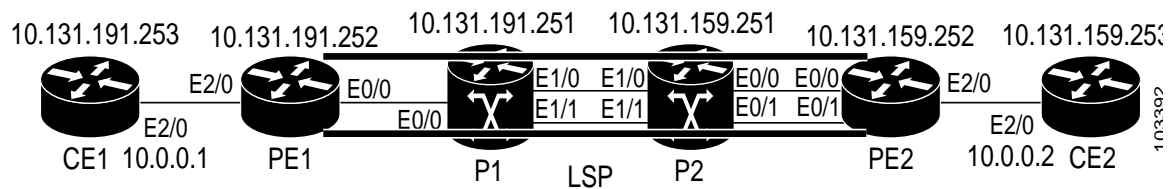
## DETAILED STEPS

<b>Step 1</b>	<pre>enable</pre> <p><b>Example:</b> Router&gt; enable</p>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<pre>show mpls l2transport binding</pre> <p><b>Example:</b> Router# show mpls l2transport binding</p>	Displays VC label binding information.
<b>Step 3</b>	<pre>exit</pre> <p><b>Example:</b> Router# exit</p>	Returns to user EXEC mode.

## Configuration Examples for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

Examples for the MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature are based on the sample topology shown in [Figure 5](#).

**Figure 5** Sample Topology for Configuration Examples



This section contains the following configuration examples:

- [Enabling Compatibility Between the MPLS LSP and Ping or Traceroute Implementation: Example, page 31](#)
- [Validating an FEC by Using MPLS LSP Ping and LSP Traceroute: Example, page 31](#)
- [Using DSCP to Request a Specific Class of Service in an Echo Reply: Example, page 32](#)
- [Controlling How a Responding Router Replies to an MPLS Echo Request: Example, page 32](#)
- [Preventing Loops when Using MPLS LSP Ping and LSP Traceroute Command Options: Example, page 32](#)
- [Detecting LSP Breaks: Example, page 36](#)
- [Viewing the AToM VCCV Capabilities Advertised to and Received from the Peer: Example, page 57](#)

## Enabling Compatibility Between the MPLS LSP and Ping or Traceroute Implementation: Example

The following example shows how to configure MPLS multipath LSP traceroute to interoperate with a vendor implementation that does not interpret RFC 4379 as Cisco does:

```
configure terminal
!
mpls oam
  echo revision 4
  no echo vendor-extension
exit
```

The default echo revision number is 4, which corresponds to the IEFT draft 11.

## Validating an FEC by Using MPLS LSP Ping and LSP Traceroute: Example

This section describes the following procedures:

- [Validating an LDP IPv4 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute: Example, page 31](#)
- [Validating a Layer 2 FEC by Using MPLS LSP Ping: Example, page 31](#)

### Validating an LDP IPv4 FEC by Using MPLS LSP Ping and MPLS LSP Traceroute: Example

The following example shows how to use the **ping mpls** command to test connectivity of an IPv4 LDP LSP:

```
Router# ping mpls ipv4 10.131.191.252/32 repeat 5 exp 5 verbose
```

Sending 5, 100-byte MPLS Echos to 10.131.191.252, timeout is 2 seconds:

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
! 10.131.191.230, return code 3
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 100/10

### Validating a Layer 2 FEC by Using MPLS LSP Ping: Example

The following example validates a Layer 2 FEC:

```
Router# ping mpls pseudowire 10.10.10.15 108 vc-id 333
```

Sending 5, 100-byte MPLS Echos to 10.10.10.15,  
timeout is 2 seconds, send interval is 0 msec:

```

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
       'L' - labeled output interface, 'B' - unlabeled output interface,
       'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
       'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
       'P' - no rx intf label prot, 'p' - premature termination of LSP,
       'R' - transit router, 'I' - unknown upstream index,
       'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/32/40 ms PE-802#

```

## Using DSCP to Request a Specific Class of Service in an Echo Reply: Example

The following example shows how to use DSCP to request a specific CoS in an echo reply:

```
Router# ping mpls ipv4 10.131.159.252/32 reply dscp 50
```

```

<0-63> Differentiated services codepoint value
af11    Match packets with AF11 dscp (001010)
af12    Match packets with AF12 dscp (001100)
af13    Match packets with AF13 dscp (001110)
af21    Match packets with AF21 dscp (010010)
af22    Match packets with AF22 dscp (010100)
af23    Match packets with AF23 dscp (010110)
af31    Match packets with AF31 dscp (011010)
af32    Match packets with AF32 dscp (011100)
af33    Match packets with AF33 dscp (011110)
af41    Match packets with AF41 dscp (100010)
af42    Match packets with AF42 dscp (100100)
af43    Match packets with AF43 dscp (100110)
cs1     Match packets with CS1(precedence 1) dscp (001000)
cs2     Match packets with CS2(precedence 2) dscp (010000)
cs3     Match packets with CS3(precedence 3) dscp (011000)
cs4     Match packets with CS4(precedence 4) dscp (100000)
cs5     Match packets with CS5(precedence 5) dscp (101000)
cs6     Match packets with CS6(precedence 6) dscp (110000)
cs7     Match packets with CS7(precedence 7) dscp (111000)
default Match packets with default dscp (000000)
ef      Match packets with EF dscp (101110)

```

## Controlling How a Responding Router Replies to an MPLS Echo Request: Example

The following example checks MPLS LSP connectivity by using ipv4 reply mode:

```
Router# ping mpls ipv4 10.131.191.252/32 reply mode ipv4
```

## Preventing Loops when Using MPLS LSP Ping and LSP Traceroute Command Options: Example

This section contains the following examples:

- [Possible Loops with MPLS LSP Ping: Example, page 33](#)
- [Possible Loop with MPLS LSP Traceroute: Example, page 34](#)

## Possible Loops with MPLS LSP Ping: Example

The following example shows how a loop operates if you use the following **ping mpls** command:

```
Router# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.2 1 repeat 2
sweep 1450 1475 25
```

Sending 2, [1450..1500]-byte MPLS Echos to 10.131.159.251/32,  
timeout is 2 seconds, send interval is 0 msec:

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

Destination address 127.0.0.1

!  
!

Destination address 127.0.0.2

!  
!

Destination address 127.0.0.1

!  
!

Destination address 127.0.0.2

!  
!

A **ping mpls** command is sent for each packet size range for each destination address until the end address is reached. For this example, the loop continues in the same manner until the destination address, 127.0.0.5, is reached. The sequence continues until the number is reached that you specified with the **repeat count** keyword and argument. For this example, the repeat count is 2. The MPLS LSP ping loop sequence is as follows:

```
repeat = 1
  destination address 1 (address-start)
    for (size from sweep minimum to maximum, counting by size-increment)
      send an lsp ping

  destination address 2 (address-start + address-increment)
    for (size from sweep minimum to maximum, counting by size-increment)
      send an lsp ping

  destination address 3 (address-start + address-increment + address-increment)
    for (size from sweep minimum to maximum, counting by size-increment)
      send an lsp ping
```

```

.
.
.
until destination address = address-end

.
.
.
until repeat = count 2

```

## Possible Loop with MPLS LSP Traceroute: Example

The following example shows how a loop occurs if you use the following **trace mpls** command:

```
Router# trace mpls ipv4 10.131.159.251/32 destination 127.0.0.1 127.0.0.3 1 ttl 5
```

Tracing MPLS Label Switched Path to 10.131.159.251/32, timeout is 2 seconds

Codes:

```

'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

```

Type escape sequence to abort.

```

Destination address 127.0.0.1
  0 10.131.191.230 MRU 1500 [Labels: 19 Exp: 0]
R 1 10.131.159.226 MRU 1504 [implicit-null] 40 ms
! 2 10.131.159.225 40 ms
Destination address 127.0.0.2
  0 10.131.191.230 MRU 1500 [Labels: 19 Exp: 0]
R 1 10.131.159.226 MRU 1504 [implicit-null] 40 ms
! 2 10.131.159.225 40 ms
Destination address 127.0.0.3
  0 10.131.191.230 MRU 1500 [Labels: 19 Exp: 0]
R 1 10.131.159.226 MRU 1504 [implicit-null] 40 ms
! 2 10.131.159.225 48 ms

```

An **mpls trace** command is sent for each TTL from 1 to the maximum TTL (**ttl maximum-time-to-live** keyword and argument) for each destination address until the address specified with the destination *end-address* argument is reached. In this example, the maximum TTL is 5 and the end destination address is 127.0.0.3. The MPLS LSP traceroute loop sequence is as follows:

```

destination address 1 (address-start)
  for (ttl from 1 to maximum-time-to-live)
    send an lsp trace

destination address 2 (address-start + address-increment)
  for (ttl from 1 to 5)
    send an lsp trace

destination address 3 (address-start + address-increment + address-increment)
  for (ttl from 1 to maximum-time-to-live)
    send an lsp trace
.
.
.
until destination address = 4

```

The following example shows that the trace encountered an LSP problem at the router that has an IP address of 10.6.1.6:

```
Router# traceroute mpls ipv4 10.6.7.4/32
```

```
Tracing MPLS Label Switched Path to 10.6.7.4/32, timeout is 2 seconds
```

```
Codes:
```

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
0 10.6.1.14 MRU 4470 [Labels: 22 Exp: 0]
R 1 10.6.1.5 MRU 4470 [Labels: 21 Exp: 0] 2 ms
R 2 10.6.1.6 4 ms                      <----- Router address repeated for 2nd to 30th TTL.
R 3 10.6.1.6 1 ms
R 4 10.6.1.6 1 ms
R 5 10.6.1.6 3 ms
R 6 10.6.1.6 4 ms
R 7 10.6.1.6 1 ms
R 8 10.6.1.6 2 ms
R 9 10.6.1.6 3 ms
R 10 10.6.1.6 4 ms
R 11 10.6.1.6 1 ms
R 12 10.6.1.6 2 ms
R 13 10.6.1.6 4 ms
R 14 10.6.1.6 5 ms
R 15 10.6.1.6 2 ms
R 16 10.6.1.6 3 ms
R 17 10.6.1.6 4 ms
R 18 10.6.1.6 2 ms
R 19 10.6.1.6 3 ms
R 20 10.6.1.6 4 ms
R 21 10.6.1.6 1 ms
R 22 10.6.1.6 2 ms
R 23 10.6.1.6 3 ms
R 24 10.6.1.6 4 ms
R 25 10.6.1.6 1 ms
R 26 10.6.1.6 3 ms
R 27 10.6.1.6 4 ms
R 28 10.6.1.6 1 ms
R 29 10.6.1.6 2 ms
R 30 10.6.1.6 3 ms                      <----- TTL 30.
```

If you know the maximum number of hops in your network, you can set the TTL to a lower value with the **trace mpls ttl maximum-time-to-live** command. The following example shows the same **traceroute** command as the previous example, except that this time the TTL is set to 5:

```
Router# traceroute mpls ipv4 10.6.7.4/32 ttl 5
```

```
Tracing MPLS Label Switched Path to 10.6.7.4/32, timeout is 2 seconds
```

```
Codes:
```

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```



```

Type escape sequence to abort.
 0 10.6.1.14 MRU 4470 [Labels: 22 Exp: 0]
R 1 10.6.1.5 MRU 4474 [No Label] 3 ms
R 2 10.6.1.6 4 ms <----- Router address repeated for 2nd to 5th TTL.
R 3 10.6.1.6 1 ms
R 4 10.6.1.6 3 ms
R 5 10.6.1.6 4 ms

```

## Detecting LSP Breaks: Example

This section contains the following examples:

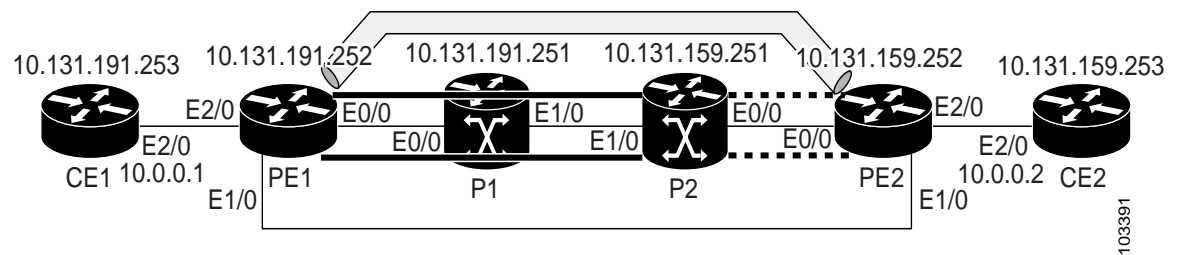
- [Troubleshooting with LSP Ping or Traceroute: Example, page 36](#)
- [MTU Discovery in an LSP: Example, page 46](#)
- [Tracking Packets Tagged as Implicit Null: Example, page 48](#)
- [Tracking Untagged Packets: Example, page 48](#)
- [Determining Why a Packet Could Not Be Sent: Example, page 49](#)
- [Detecting LSP Breaks when Load Balancing Is Enabled for IPv4 LSPs: Example, page 50](#)
- [Specifying the Interface Through Which Echo Packets Leave a Router: Example, page 52](#)
- [Pacing the Transmission of Packets: Example, page 53](#)
- [Interrogating the Transit Router for Its Downstream Information: Example, page 53](#)
- [Interrogating a Router for Its DSMAP: Example, page 55](#)
- [Requesting that a Transit Router Validate the Target FEC Stack: Example, page 56](#)
- [Enabling LSP Ping to Detect LSP Breakages Caused by Untagged Interfaces: Example, page 56](#)

## Troubleshooting with LSP Ping or Traceroute: Example

ICMP **ping** and **trace** commands are often used to help diagnose the root cause of a failure. When an LSP is broken, the packet may reach the target router by IP forwarding, thus making the ICMP ping and traceroute features unreliable for detecting MPLS forwarding problems. The MPLS LSP ping or traceroute and AToM VCCV features extend this diagnostic and troubleshooting ability to the MPLS network and handle inconsistencies (if any) between the IP and MPLS forwarding tables, inconsistencies in the MPLS control and data plane, and problems with the reply path.

Figure 6 shows a sample topology with an LDP LSP.

**Figure 6** Sample Topology with LDP LSP



This section contains the following subsections:

- [Configuration for Sample Topology, page 37](#)
- [Verification That the LSP Is Configured Correctly, page 43](#)
- [Discovery of LSP Breaks, page 44](#)

## Configuration for Sample Topology

These are sample topology configurations for the troubleshooting examples in the following sections (see [Figure 6](#)). There are the six sample router configurations.

### Router CE1 Configuration

Following is the configuration for the CE1 router:

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname CE1  
!  
boot-start-marker  
boot-end-marker  
!  
enable password lab  
!  
clock timezone EST -5  
ip subnet-zero  
!  
!  
!  
interface Loopback0  
 ip address 10.131.191.253 255.255.255.255  
 no ip directed-broadcast  
 no clns route-cache  
!  
!  
interface Ethernet2/0  
 no ip address  
 no ip directed-broadcast  
 no keepalive  
 no cdp enable  
 no clns route-cache  
!  
interface Ethernet2/0.1  
 encapsulation dot1Q 1000  
 ip address 10.0.0.1 255.255.255.0  
 no ip directed-broadcast  
!  
!  
line con 0  
 exec-timeout 0 0  
line aux 0  
line vty 0 4  
 exec-timeout 0 0  
 password lab  
 login  
!  
end
```

**Router PE1 Configuration**

Following is the configuration for the PE1 router:

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE1
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
enable password lab
!
clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
!
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!
!
!
interface Loopback0
 ip address 10.131.191.252 255.255.255.255
 no clns route-cache
!
interface Ethernet0/0
 ip address 10.131.191.230 255.255.255.252
 ip rsvp bandwidth 1500 1500
 ip rsvp signalling dscp 0
!
interface Ethernet1/0
 ip address 10.131.159.246 255.255.255.252
 shutdown
 no clns route-cache
 ip rsvp bandwidth 1500 1500
 ip rsvp signalling dscp 0
!
interface Ethernet2/0
 no ip address
 no cdp enable
 no clns route-cache
!
interface Ethernet2/0.1
 encapsulation dot1Q 1000
 xconnect 10.131.159.252 333 encapsulation mpls
!
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 10.131.159.244 0.0.0.3 area 0
 network 10.131.191.228 0.0.0.3 area 0
 network 10.131.191.232 0.0.0.3 area 0
 network 10.131.191.252 0.0.0.0 area 0
!
!

```

```

!
line con 0
  exec-timeout 0 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password lab
  login
!
!
end

```

### Router P1 Configuration

Following is the configuration for the P1 router:

```

version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P1
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
enable password lab
!
clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
!
!
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!
!
!

no clns route-cache
!
interface Loopback0
  ip address 10.131.191.251 255.255.255.255
  no clns route-cache
!
interface Ethernet0/0
  ip address 10.131.191.229 255.255.255.252
  no clns route-cache
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
interface Ethernet1/0
  ip address 10.131.159.226 255.255.255.252
  no clns route-cache
  ip rsvp bandwidth 1500 1500
  ip rsvp signalling dscp 0
!
interface Ethernet1/1
  ip address 10.131.159.222 255.255.255.252
  no clns route-cache
  ip rsvp bandwidth 1500 1500

```

```

ip rsvp signalling dscp 0
!
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 10.131.159.220 0.0.0.3 area 0
 network 10.131.159.224 0.0.0.3 area 0
 network 10.131.191.228 0.0.0.3 area 0
 network 10.131.191.251 0.0.0.0 area 0
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 0
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
end

```

### Router P2 Configuration

Following is the configuration for the P2 router:

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname P2
!
boot-start-marker
boot-end-marker
!
enable password lab
!
clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
!
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!
!
!
interface Loopback0
 ip address 10.131.159.251 255.255.255.255
 no ip directed-broadcast
!
interface Ethernet0/0
 ip address 10.131.159.229 255.255.255.252
 no ip directed-broadcast
 ip rsvp bandwidth 1500 1500
 ip rsvp signalling dscp 0
!
interface Ethernet0/1
 ip address 10.131.159.233 255.255.255.252

```

```

no ip directed-broadcast
ip rsvp signalling dscp 0
!
interface Ethernet1/0
 ip address 10.131.159.225 255.255.255.252
no ip directed-broadcast
ip rsvp bandwidth 1500 1500
ip rsvp signalling dscp 0
!
interface Ethernet1/1
 ip address 10.131.159.221 255.255.255.252
no ip directed-broadcast
ip rsvp signalling dscp 0
!
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 10.131.159.220 0.0.0.3 area 0
 network 10.131.159.224 0.0.0.3 area 0
 network 10.131.159.228 0.0.0.3 area 0
 network 10.131.159.232 0.0.0.3 area 0
 network 10.131.159.251 0.0.0.0 area 0
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
end

```

### Router PE2 Configuration

Following is the configuration for the PE2 router:

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname PE2
!
boot-start-marker
boot-end-marker
!
logging snmp-authfail
enable password lab
!
clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
!
mpls ldp discovery targeted-hello accept
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!
!

```

```

!
interface Loopback0
 ip address 10.131.159.252 255.255.255.255
 no clns route-cache
!
interface Ethernet0/0
 ip address 10.131.159.230 255.255.255.252
 no clns route-cache
 ip rsvp bandwidth 1500 1500
 ip rsvp signalling dscp 0
!
interface Ethernet0/1
 ip address 10.131.159.234 255.255.255.252
 no clns route-cache
 ip rsvp bandwidth 1500 1500
 ip rsvp signalling dscp 0
!
interface Ethernet1/0
 ip address 10.131.159.245 255.255.255.252
 mpls ip
 no clns route-cache
!
interface Ethernet3/0
 no ip address
 no cdp enable
 no clns route-cache
!
interface Ethernet3/0.1
 encapsulation dot1Q 1000
 no snmp trap link-status
 no cdp enable
 xconnect 10.131.191.252 333 encapsulation mpls
!
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback0
 network 10.131.122.0 0.0.0.3 area 0
 network 10.131.159.228 0.0.0.3 area 0
 network 10.131.159.232 0.0.0.3 area 0
 network 10.131.159.236 0.0.0.3 area 0
 network 10.131.159.244 0.0.0.3 area 0
 network 10.131.159.252 0.0.0.0 area 0
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
!
end

```

### Router CE2 Configuration

Following is the configuration for the CE2 router:

```

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec

```

```

no service password-encryption
!
hostname CE2
!
boot-start-marker
boot-end-marker
!
enable password lab
!
clock timezone EST -5
ip subnet-zero
ip cef
no ip domain-lookup
!
!
interface Loopback0
 ip address 10.131.159.253 255.255.255.255
 no ip directed-broadcast
 no clns route-cache
!
interface Ethernet3/0
 no ip address
 no ip directed-broadcast
 no keepalive
 no cdp enable
 no clns route-cache
!
interface Ethernet3/0.1
 encapsulation dot1Q 1000
 ip address 10.0.0.2 255.255.255.0
 no ip directed-broadcast
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password lab
 login
!
end

```

## Verification That the LSP Is Configured Correctly

Use the output from the **show** commands in this section to verify that the LSP is configured correctly.

A **show mpls forwarding-table** command shows that tunnel 1 is in the MPLS forwarding table.

```
PE1# show mpls forwarding-table 10.131.159.252
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
22	18 [T]	10.131.159.252/32 0	Tu1	point2point	

```
[T] Forwarding through a TSP tunnel.
View additional tagging info with the 'detail' option
```

A **trace mpls** command issued at PE1 verifies that packets with 16 as the outermost label and 18 as the end-of-stack label are forwarded from PE1 to PE2.

```
PE1# trace mpls ipv4 10.131.159.252/32
```



Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
0 10.131.191.252 MRU 1496 [Labels: 16/18 Exp: 0/0] L 1 10.131.191.229
MRU 1508 [Labels: 18 Exp: 0] 0 ms L 2 10.131.159.225
MRU 1504 [Labels: implicit-null Exp: 0] 0 ms ! 3 10.131.159.234 20 ms
PE1#
```

The MPLS LSP Traceroute to PE2 is successful, as indicated by the exclamation point (!).

## Discovery of LSP Breaks

Use the output of the commands in this section to discover LSP breaks.

An LDP target session is established between routers PE1 and P2, as shown in the output of the following **show mpls ldp discovery** command:

PE1# **show mpls ldp discovery**

```
Local LDP Identifier:
 10.131.191.252:0
Discovery Sources:
Interfaces:
  Ethernet0/0 (ldp): xmit/recv
    LDP Id: 10.131.191.251:0
  Tunnel1 (ldp): Targeted -> 10.131.159.251
Targeted Hellos:
 10.131.191.252 -> 10.131.159.252 (ldp): active/passive, xmit/recv
    LDP Id: 10.131.159.252:0
 10.131.191.252 -> 10.131.159.251 (ldp): active, xmit/recv
    LDP Id: 10.131.159.251:0
```

Enter the following command on the P2 router in global configuration mode:

P2(config)# **no mpls ldp discovery targeted-hello accept**

The LDP configuration change causes the targeted LDP session between the headend and tailend of the TE tunnel to go down. Labels for IPv4 prefixes learned by P2 are not advertised to PE1. Thus, all IP prefixes reachable by P2 are reachable by PE1 only through IP (not MPLS). In other words, packets destined for those prefixes through Tunnel 1 at PE1 will be IP switched at P2 (which is undesirable).

The following **show mpls ldp discovery** command shows that the LDP targeted session is down:

PE1# **show mpls ldp discovery**

```
Local LDP Identifier:
 10.131.191.252:0
Discovery Sources:
Interfaces:
  Ethernet0/0 (ldp): xmit/recv
    LDP Id: 10.131.191.251:0
  Tunnel1 (ldp): Targeted -> 10.131.159.251
Targeted Hellos:
 10.131.191.252 -> 10.131.159.252 (ldp): active/passive, xmit/recv
    LDP Id: 10.131.159.252:0
 10.131.191.252 -> 10.131.159.251 (ldp): active, xmit
```

Enter the **show mpls forwarding-table** command at the PE1 router. The display shows that the outgoing packets are untagged as a result of the LDP configuration changes.

```
PE1# show mpls forwarding-table 10.131.159.252
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
22	Untagged[T]	10.131.159.252/32	0	Tu1	point2point

```
[T] Forwarding through a TSP tunnel.
View additional tagging info with the 'detail' option
```

A **ping mpls** command entered at the PE1 router displays the following:

```
PE1# ping mpls ipv4 10.131.159.252/32 repeat 1
```

```
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
timeout is 2 seconds, send interval is 0 msec:
```

```
Codes:
```

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
R
```

```
Success rate is 0 percent (0/1)
```

The **ping mpls** command fails. The R indicates that the sender of the MPLS echo reply had a routing entry but no MPLS FEC. Entering the **verbose** keyword with the **ping mpls** command displays the MPLS LSP echo reply sender address and the return code. You should be able to determine where the breakage occurred by telnetting to the replying router and inspecting its forwarding and label tables. You might need to look at the neighboring upstream router as well, because the breakage might be on the upstream router.

```
PE1# ping mpls ipv4 10.131.159.252/32 repeat 1 verbose
```

```
Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
timeout is 2 seconds, send interval is 0 msec:
```

```
Codes:
```

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
R 10.131.159.225, return code 6
```

```
Success rate is 0 percent (0/1)
```

Alternatively, use the **LSP traceroute** command to figure out which router caused the breakage. In the following example, for subsequent values of TTL greater than 2, the same router keeps responding (10.131.159.225). This suggests that the MPLS echo request keeps getting processed by the router regardless of the TTL. Inspection of the label stack shows that P1 pops the last label and forwards the

packet to P2 as an IP packet. This explains why the packet keeps getting processed by P2. MPLS echo request packets cannot be forwarded by use of the destination address in the IP header because the address is set to a 127/8 address.

```
PE1# trace mpls ipv4 10.131.159.252/32 ttl 5
```

Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
0 10.131.191.230 MRU 1496 [Labels: 22/19 Exp: 0/0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 40 ms
R 2 10.131.159.229 MRU 1504 [implicit-null] 28 ms
! 3 10.131.159.230 40 ms
pe1#
```

## MTU Discovery in an LSP: Example

The following example shows the results of a **trace mpls** command when the LSP is formed with labels created by LDP:

```
PE1# trace mpls ipv4 10.131.159.252/32
```

Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
0 10.131.191.230 MRU 1496 [Labels: 22/19 Exp: 0/0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 40 ms
R 2 10.131.159.229 MRU 1504 [implicit-null] 28 ms
! 3 10.131.159.230 40 ms
pe1#
```

You can determine the MRU for the LSP at each hop through the use of the **show mpls forwarding detail** command:

```
PE1# show mpls forwarding 10.131.159.252 detail
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
22	19	10.131.159.252/32	0	Tul	point2point
MAC/Encaps=14/22, MRU=1496, Tag Stack{22 19}, via Et0/0					
AABBCC009700AABBCC0098008847 0001600000013000					
No output feature configured					

To determine how large an echo request will fit on the LSP, first calculate the size of the IP MTU by using the **show interface interface-name** command:

```
PE1# show interface e0/0
```

```

Ethernet0/0 is up, line protocol is up
  Hardware is Lance, address is aabb.cc00.9800 (bia aabb.cc00.9800)
  Internet address is 10.131.191.230/30
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:01, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    377795 packets input, 33969220 bytes, 0 no buffer
    Received 231137 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    441772 packets output, 40401350 bytes, 0 underruns
    0 output errors, 0 collisions, 10 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out

```

The IP MTU in the **show interface interface-name** example is 1500 bytes. Subtract the number of bytes corresponding to the label stack from the MTU number. The output of the **show mpls forwarding** command indicates that the Tag stack consists of one label (21). Therefore, the largest MPLS echo request packet that can be sent in the LSP is  $1500 - (2 \times 4) = 1492$ .

You can validate this by using the following **mpls ping** command:

```
PE1# ping mpls ipv4 10.131.159.252/32 sweep 1492 1500 1 repeat 1
```

```

Sending 1, [1492..1500]-byte MPLS Echos to 10.131.159.252/32,
  timeout is 2 seconds, send interval is 0 msec:

```

Codes:

```

'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

```

Type escape sequence to abort.

```
!QQQQQQQ
```

```
Success rate is 11 percent (1/9), round-trip min/avg/max = 40/40/40 ms
```

In this command, echo packets that have a range in size from 1492 to 1500 bytes are sent to the destination address. Only packets of 1492 bytes are sent successfully, as indicated by the exclamation point (!). Packets of byte sizes 1493 to 1500 are source-quenched, as indicated by the Qs.

You can pad an MPLS echo request so that a payload of a given size can be tested. The pad TLV is useful when you use the MPLS echo request to discover the MTU that is supportable by an LSP. MTU discovery is extremely important for applications like AToM that contain non-IP payloads that cannot be fragmented.

## Tracking Packets Tagged as Implicit Null: Example

In the following example, Tunnel 1 is shut down, and only an LSP formed with LDP labels is established. An implicit null is advertised between the P2 and PE2 routers. Entering an MPLS LSP traceroute command at the PE1 router results in the following output that shows that packets are forwarded from P2 to PE2 with an implicit-null label. Address 10.131.159.229 is configured for the P2 Ethernet 0/0 out interface for the PE2 router.

```
PE1# trace mpls ipv4 10.131.159.252/32
```

```
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
```

```
Codes:
```

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
0 10.131.191.230 MRU 1496 [Labels: 22/19 Exp: 0/0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 40 ms
R 2 10.131.159.229 MRU 1504 [implicit-null] 28 ms
! 3 10.131.159.230 40 ms
pe1#
```

## Tracking Untagged Packets: Example

Untagged cases are valid configurations for IGP LSPs that could cause problems for MPLS VPNs.

A **show mpls forwarding-table** command and a **show mpls ldp discovery** command issued at the P2 router show that LDP is properly configured:

```
P2# show mpls forwarding-table 10.131.159.252
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
19	Pop tag	10.131.159.252/32	0	Et0/0	10.131.159.230

```
P2# show mpls ldp discovery
```

```
Local LDP Identifier:
 10.131.159.251:0
Discovery Sources:
Interfaces:
 Ethernet0/0 (ldp): xmit/recvd
   LDP Id: 10.131.159.252:0
 Ethernet1/0 (ldp): xmit/recvd
   LDP Id: 10.131.191.251:0
```

The **show mpls ldp discovery** command output shows that Ethernet interface 0/0, which connects PE2 to P2, is sending and receiving packets.

If a **no mpls ip** command is entered on Ethernet interface 0/0, this could prevent an LDP session between the P2 and PE2 routers from being established. A **show mpls ldp discovery** command entered on the PE router shows that the MPLS LDP session with the PE2 router is down.

```
P2# show mpls ldp discovery
```

```
Local LDP Identifier:
 10.131.159.251:0
```

```

Discovery Sources:
Interfaces:
  Ethernet0/0 (ldp): xmit
  Ethernet1/0 (ldp): xmit/recv
  LDP Id: 10.131.191.251:0

```

If the MPLS LDP session to PE2 goes down, the LSP to 10.131.159.252 becomes untagged, as shown by the **show mpls forwarding-table** command:

```
P2# show mpls forwarding-table 10.131.159.252/32
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
19	Untagged	10.131.159.252/32	864	Et0/0	10.131.159.230

Untagged cases would provide an MPLS LSP traceroute reply with packets tagged with No Label, as shown in the following display. You may need to reestablish an MPLS LSP session from interface P2 to PE2 by entering an **mpls ip** command on the output interface from P2 to PE2, which is Ethernet 0/0 in this example:

```
PE1# trace mpls ipv4 10.131.159.252/32
```

```
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
```

```
Codes:
```

```

'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

```

```
Type escape sequence to abort.
```

```

0 10.131.191.230 MRU 1500 [Labels: 20 Exp: 0]
R 1 10.131.159.226 MRU 1500 [Labels: 19 Exp: 0] 80 ms
R 2 10.131.159.229 MRU 1504 [No Label] 28 ms      <---No MPLS session from P2 to PE2.
! 3 10.131.159.230 40 ms

```

## Determining Why a Packet Could Not Be Sent: Example

The following example shows a **ping mpls** command when an MPLS echo request is not sent. The transmission failure is shown by the returned Qs.

```
PE1# ping mpls ipv4 10.0.0.1/32
```

```

Sending 5, 100-byte MPLS Echos to 10.0.0.1/32,
  timeout is 2 seconds, send interval is 0 msec:

```

```
Codes:
```

```

'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

```

```
Type escape sequence to abort.
```

```
QQQQQ
```

```
Success rate is 0 percent (0/5)
```

The following **show mpls forwarding-table** command and **show ip route** command demonstrate that the IPv4 address (10.0.0.1) address is not in the LFIB or RIB routing table. Therefore, the MPLS echo request is not sent.

```
PE1# show mpls forwarding-table 10.0.0.1

Local  Outgoing  Prefix          Bytes tag  Outgoing     Next Hop
tag    tag or VC   or Tunnel Id    switched   interface

PE1# show ip route 10.0.0.1

% Subnet not in table
```

## Detecting LSP Breaks when Load Balancing Is Enabled for IPv4 LSPs: Example

In the following examples, different paths are followed to the same destination. The output from these examples demonstrates that load balancing occurs between the originating router and the target router.

To ensure that Ethernet interface 1/0 on the PE1 router is operational, enter the following commands on the PE1 router:

```
PE1# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

PE1(config)# interface ethernet 1/0

PE1(config-if)# no shutdown

PE1(config-if)# end

*Dec 31 19:14:10.034: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Dec 31 19:14:11.054: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0,
changed state to upend
PE1#
*Dec 31 19:14:12.574: %SYS-5-CONFIG_I: Configured from console by console
*Dec 31 19:14:19.334: %OSPF-5-ADJCHG: Process 1, Nbr 10.131.159.252 on Ethernet1/0
from LOADING to FULL, Loading Done
PE1#
```

The following **show mpls forwarding-table** command displays the possible outgoing interfaces and next hops for the prefix 10.131.159.251/32:

```
PE1# show mpls forwarding-table 10.131.159.251/32

Local  Outgoing  Prefix          Bytes tag  Outgoing     Next Hop
tag    tag or VC   or Tunnel Id    switched   interface

21     19         10.131.159.251/32 0           Et0/0       10.131.191.229
20     20         10.131.159.251/32 0           Et1/0       10.131.159.245
```

The following **ping mpls** command to 10.131.159.251/32 with a destination UDP address of 127.0.0.1 shows that the selected path has a path index of 0:

```
Router# ping mpls ipv4 10.131.159.251/32 destination 127.0.0.1/32
```

```
Sending 1, 100-byte MPLS Echos to 10.131.159.251/32,
timeout is 2 seconds, send interval is 0 msec:
```

Codes:

```
'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
```

'P' - no rx intf label prot, 'p' - premature termination of LSP,  
 'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!

Success rate is 100 percent (1/1), round-trip min/avg/max = 40/40/40 ms

PE1#

\*Dec 29 20:42:40.638: LSPV: Echo Request sent on IPV4 LSP, load\_index 2, pathindex 0, size 100

\*Dec 29 20:42:40.638: 46 00 00 64 00 00 40 00 FF 11 9D 03 0A 83 BF FC

\*Dec 29 20:42:40.638: 7F 00 00 01 94 04 00 00 0D AF 0D AF 00 4C 14 70

\*Dec 29 20:42:40.638: 00 01 00 00 01 02 00 00 1A 00 00 1C 00 00 00 01

\*Dec 29 20:42:40.638: C3 9B 10 40 A3 6C 08 D4 00 00 00 00 00 00 00 00

\*Dec 29 20:42:40.638: 00 01 00 09 00 01 00 05 0A 83 9F FB 20 00 03 00

\*Dec 29 20:42:40.638: 13 01 AB CD AB CD AB CD AB CD AB CD AB CD

\*Dec 29 20:42:40.638: AB CD AB CD

\*Dec 29 20:42:40.678: LSPV: Echo packet received: src 10.131.159.225, dst 10.131.191.252, size 74

\*Dec 29 20:42:40.678: AA BB CC 00 98 01 AA BB CC 00 FC 01 08 00 45 C0

\*Dec 29 20:42:40.678: 00 3C 32 D6 00 00 FD 11 15 37 0A 83 9F E1 0A 83

\*Dec 29 20:42:40.678: BF FC 0D AF 0D AF 00 28 D1 85 00 01 00 00 02 02

\*Dec 29 20:42:40.678: 03 00 1A 00 00 1C 00 00 00 01 C3 9B 10 40 A3 6C

\*Dec 29 20:42:40.678: 08 D4 C3 9B 10 40 66 F5 C3 C8

The following **ping mpls** command to 10.131.159.251/32 with a destination UDP address of 127.0.0.3 shows that the selected path has a path index of 1:

PE1# **ping mpls ipv4 10.131.159.251/32 destination 127.0.0.3/32**

Sending 1, 100-byte MPLS Echos to 10.131.159.251/32,

timeout is 2 seconds, send interval is 0 msec:

Codes:

'!' - success, 'Q' - request not sent, '.' - timeout,

'L' - labeled output interface, 'B' - unlabeled output interface,

'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,

'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,

'P' - no rx intf label prot, 'p' - premature termination of LSP,

'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

!

Success rate is 100 percent (1/1), round-trip min/avg/max = 40/40/40 ms

PE1#

\*Dec 29 20:43:09.518: LSPV: Echo Request sent on IPV4 LSP, load\_index 13, pathindex 1, size 100

\*Dec 29 20:43:09.518: 46 00 00 64 00 00 40 00 FF 11 9D 01 0A 83 BF FC

\*Dec 29 20:43:09.518: 7F 00 00 03 94 04 00 00 0D AF 0D AF 00 4C 88 58

\*Dec 29 20:43:09.518: 00 01 00 00 01 02 00 00 38 00 00 1D 00 00 00 01

\*Dec 29 20:43:09.518: C3 9B 10 5D 84 B3 95 84 00 00 00 00 00 00 00 00

\*Dec 29 20:43:09.518: 00 01 00 09 00 01 00 05 0A 83 9F FB 20 00 03 00

\*Dec 29 20:43:09.518: 13 01 AB CD AB CD AB CD AB CD AB CD AB CD

\*Dec 29 20:43:09.518: AB CD AB CD

\*Dec 29 20:43:09.558: LSPV: Echo packet received: src 10.131.159.229, dst 10.131.191.252, size 74

\*Dec 29 20:43:09.558: AA BB CC 00 98 01 AA BB CC 00 FC 01 08 00 45 C0

\*Dec 29 20:43:09.558: 00 3C 32 E9 00 00 FD 11 15 20 0A 83 9F E5 0A 83

\*Dec 29 20:43:09.558: BF FC 0D AF 0D AF 00 28 D7 57 00 01 00 00 02 02

\*Dec 29 20:43:09.558: 03 00 38 00 00 1D 00 00 00 01 C3 9B 10 5D 84 B3

\*Dec 29 20:43:09.558: 95 84 C3 9B 10 5D 48 3D 50 78

To see the actual path chosen, enter the **debug mpls lsvp** command with the **packet** and **data** keywords.



**Note**

The load balancing algorithm attempts to uniformly distribute packets across the available output paths by hashing based on the IP header source and destination addresses. The selection of the *address-start*, *address-end*, and *address-increment* arguments for the **destination** keyword may not provide the expected results.

## Specifying the Interface Through Which Echo Packets Leave a Router: Example

The following example tests load balancing from the upstream router:

```
Router# ping mpls ipv4 10.131.161.251/32 ttl 1 repeat 1 dsmap hashkey ipv4 bitmap 8
```

```
Sending 1, 100-byte MPLS Echos to 10.131.161.251/32,
  timeout is 2 seconds, send interval is 0 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
L
```

```
Echo Reply received from 10.131.131.2
```

```
DSMAP 0, DS Router Addr 10.131.141.130, DS Intf Addr 10.131.141.130
```

```
Depth Limit 0, MRU 1500 [Labels: 54 Exp: 0]
```

```
Multipath Addresses:
```

```
127.0.0.3      127.0.0.5      127.0.0.7      127.0.0.8
```

```
DSMAP 1, DS Router Addr 10.131.141.2, DS Intf Addr 10.131.141.2
```

```
Depth Limit 0, MRU 1500 [Labels: 40 Exp: 0]
```

```
Multipath Addresses:
```

```
127.0.0.1      127.0.0.2      127.0.0.4      127.0.0.6
```

The following example validates that the transit router reported the proper results by determining the Echo Reply sender address two hops away and checking the rx label advertised upstream:

```
Success rate is 0 percent (0/1)
```

```
Router# trace mpls ipv4 10.131.161.251/32 destination 127.0.0.6 ttl 2
```

```
Tracing MPLS Label Switched Path to 10.131.161.251/32, timeout is 2 seconds
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
0 10.131.131.1 10.131.131.2 MRU 1500 [Labels: 37 Exp: 0]
```

```
L 1 10.131.131.2 10.131.141.2 MRU 1500 [Labels: 40 Exp: 0] 0 ms, ret code 8
```

```
L 2 10.131.141.2 10.131.150.2 MRU 1504 [Labels: implicit-null Exp: 0] 0 ms, ret code 8
```

```
Router#
```

```
Router# telnet 10.131.141.2
```

```
Trying 10.131.141.2 ... Open
```

```
User Access Verification
```

```
Password:
Router> en
```

The following example shows how the **output interface** keyword forces an LSP traceroute out Ethernet interface 0/0:

```
Router# show mpls forwarding-table 10.131.159.251
```

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
20	19	10.131.159.251/32	0	Et1/0	10.131.159.245
	18	10.131.159.251/32	0	Et0/0	10.131.191.229

```
Router# trace mpls ipv4 10.131.159.251/32
```

```
Tracing MPLS Label Switched Path to 10.131.159.251/32, timeout is 2 seconds
```

```
Type escape sequence to abort.
```

```
  0 10.131.159.246 MRU 1500 [Labels: 19 Exp: 0]
L 1 10.131.159.245 MRU 1504 [Labels: implicit-null Exp: 0] 4 ms
! 2 10.131.159.229 20 ms
```

```
Router# trace mpls ipv4 10.131.159.251/32 output-interface ethernet0/0
```

```
Tracing MPLS Label Switched Path to 10.131.159.251/32, timeout is 2 seconds
```

```
Type escape sequence to abort.
```

```
  0 10.131.191.230 MRU 1500 [Labels: 18 Exp: 0]
L 1 10.131.191.229 MRU 1504 [Labels: implicit-null Exp: 0] 0 ms
! 2 10.131.159.225 1 ms
```

## Pacing the Transmission of Packets: Example

The following example shows the pace of the transmission of packets:

```
Router# ping mpls ipv4 10.5.5.5/32 interval 100
```

```
Sending 5, 100-byte MPLS Echos to 10.5.5.5/32,
timeout is 2 seconds, send interval is 100 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0
```

```
Type escape sequence to abort.
```

```
!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/36 ms PE-802
```

## Interrogating the Transit Router for Its Downstream Information: Example

The following example shows sample output when a router with two output paths is interrogated:

```
Router# ping mpls ipv4 10.161.251/32 ttl 4 repeat 1 dsmap hashkey ipv4 bitmap 16
```

```
Sending 1, 100-byte MPLS Echos to 10.131.161.251/32,
timeout is 2 seconds, send interval is 0 msec:
```

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
```

'L' - labeled output interface, 'B' - unlabeled output interface,  
 'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,  
 'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,  
 'P' - no rx intf label prot, 'p' - premature termination of LSP,  
 'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

L

Echo Reply received from 10.131.131.2

DSMAP 0, DS Router Addr 10.131.141.130, DS Intf Addr 10.131.141.130  
 Depth Limit 0, MRU 1500 [Labels: 54 Exp: 0]  
 Multipath Addresses:  
     127.0.0.3        127.0.0.6        127.0.0.9        127.0.0.10  
     127.0.0.12      127.0.0.13      127.0.0.14      127.0.0.15  
     127.0.0.16

DSMAP 1, DS Router Addr 10.131.141.2, DS Intf Addr 10.131.141.2  
 Depth Limit 0, MRU 1500 [Labels: 40 Exp: 0]  
 Multipath Addresses:  
     127.0.0.1        127.0.0.2        127.0.0.4        127.0.0.5  
     127.0.0.7        127.0.0.8        127.0.0.11

Success rate is 0 percent (0/1)

The multipath addresses cause a packet to transit to the router with the output label stack. The **ping mpls** command is useful for determining the number of output paths, but when the router is more than one hop away a router cannot always use those addresses to get the packet to transit through the router being interrogated. This situation exists because the change in the IP header destination address may cause the packet to be load-balanced differently by routers between the source router and the responding router. Load balancing is affected by the source address in the IP header. The following example tests load-balancing reporting from the upstream router:

Router# **ping mpls ipv4 10.131.161.251/32 ttl 1 repeat 1 dsmap hashkey ipv4 bitmap 8**

Sending 1, 100-byte MPLS Echos to 10.131.161.251/32,  
 timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,  
 'L' - labeled output interface, 'B' - unlabeled output interface,  
 'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,  
 'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,  
 'P' - no rx intf label prot, 'p' - premature termination of LSP,  
 'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.

L

Echo Reply received from 10.131.131.2

DSMAP 0, DS Router Addr 10.131.141.130, DS Intf Addr 10.131.141.130  
 Depth Limit 0, MRU 1500 [Labels: 54 Exp: 0]  
 Multipath Addresses:  
     127.0.0.3        127.0.0.5        127.0.0.7        127.0.0.8

DSMAP 1, DS Router Addr 10.131.141.2, DS Intf Addr 10.131.141.2  
 Depth Limit 0, MRU 1500 [Labels: 40 Exp: 0]  
 Multipath Addresses:  
     127.0.0.1        127.0.0.2        127.0.0.4        127.0.0.6

To validate that the transit router reported the proper results, determine the Echo Reply sender address that is two hops away and consistently check the rx label that is advertised upstream. The following is sample output:

Success rate is 0 percent (0/1)

```

Router# trace mpls ipv4 10.131.161.251/32 destination 127.0.0.6 ttl 2

Tracing MPLS Label Switched Path to 10.131.161.251/32, timeout is 2 seconds

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
 0 10.131.131.1 10.131.131.2 MRU 1500 [Labels: 37 Exp: 0]
L 1 10.131.131.2 10.131.141.2 MRU 1500 [Labels: 40 Exp: 0] 0 ms, ret code 8
L 2 10.131.141.2 10.131.150.2 MRU 1504 [Labels: implicit-null Exp: 0] 0 ms, ret code 8
Router#
Router# telnet 10.131.141.2
Trying 10.131.141.2 ... Open

User Access Verification

Password:
Router> en

Router# show mpls forwarding-table 10.131.161.251

Local   Outgoing   Prefix           Bytes tag  Outgoing     Next Hop
tag     tag or VC  or Tunnel Id     switched   interface
40      Pop tag    10.131.161.251/32 268        Et1/0        10.131.150.2
Router#

```

## Interrogating a Router for Its DSMAP: Example

The following example interrogates the software and hardware forwarding layer for their depth limit that needs to be returned in the DSMAP TLV.

```

Router# ping mpls ipv4 10.131.159.252/32 ttl 1 dsmap

Sending 1, 100-byte MPLS Echos to 10.131.159.252/32,
        timeout is 2 seconds, send interval is 0 msec:

Codes:
        '!' - success, 'Q' - request not sent, '.' - timeout,
        'L' - labeled output interface, 'B' - unlabeled output interface,
        'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
        'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
        'P' - no rx intf label prot, 'p' - premature termination of LSP,
        'R' - transit router, 'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
L
Echo Reply received from 10.131.191.229
  DSMAP 0, DS Router Addr 10.131.159.225, DS Intf Addr 10.131.159.225
    Depth Limit 0, MRU 1508 [Labels: 18 Exp: 0]
    Multipath Addresses:
      127.0.0.1      127.0.0.2      127.0.0.3      127.0.0.4
      127.0.0.5      127.0.0.6      127.0.0.7      127.0.0.8
      127.0.0.9      127.0.0.10     127.0.0.11     127.0.0.12
      127.0.0.13     127.0.0.14     127.0.0.15     127.0.0.16
      127.0.0.17     127.0.0.18     127.0.0.19     127.0.0.20
      127.0.0.21     127.0.0.22     127.0.0.23     127.0.0.24
      127.0.0.25     127.0.0.26     127.0.0.27     127.0.0.28

```

```

127.0.0.29      127.0.0.30      127.0.0.31      127.0.0.32
Success rate is 0 percent (0/1)

```

## Requesting that a Transit Router Validate the Target FEC Stack: Example

The following example causes a transit router to validate the target FEC stack by which an LSP to be tested is identified:

```
Router# trace mpls ipv4 10.5.5.5/32 flags fec
```

```
Tracing MPLS Label Switched Path to 10.5.5.5/32, timeout is 2 seconds
```

```

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

```

Type escape sequence to abort.

```

0 10.2.3.2 10.2.3.3 MRU 1500 [Labels: 19 Exp: 0] L 1 10.2.3.3 10.3.4.4 MRU 1500 [Labels:
19 Exp: 0] 40 ms, ret code 8 L 2 10.3.4.4 10.4.5.5 MRU 1504 [Labels: implicit-null Exp: 0]
32 ms, ret code 8 ! 3 10.4.5.5 40 ms, ret code 3

```

```
Router# ping mpls ipv4 10.5.5.5/32
```

```

Sending 5, 100-byte MPLS Echos to 10.5.5.5/32
timeout is 2 seconds, send interval is 0 msec:

```

```

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'I' - unknown upstream index,
'X' - unknown return code, 'x' - return code 0

```

Type escape sequence to abort.

```

! size 100, reply addr 10.4.5.5, return code 3
! size 100, reply addr 10.4.5.5, return code 3
! size 100, reply addr 10.4.5.5, return code 3
! size 100, reply addr 10.4.5.5, return code 3
! size 100, reply addr 10.4.5.5, return code 3

```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/31/32 ms
```

## Enabling LSP Ping to Detect LSP Breakages Caused by Untagged Interfaces: Example

The following example shows the extra label that is added to the end of the label stack when there is explicit-null label shimming:

```
Router# trace mpls ipv4 10.131.159.252/32 force-explicit-null
```

```
Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds
```

Codes:

```

'!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0

```

Type escape sequence to abort.

```
0 10.131.191.252 MRU 1492 [Labels: 16/18/explicit-null Exp: 0/0/0]
L 1 10.131.191.229 MRU 1508 [Labels: 18/explicit-null Exp: 0/0] 0 ms
L 2 10.131.159.225 MRU 1508 [Labels: explicit-null Exp: 0] 0 ms
! 3 10.131.159.234 4 ms
```

The following example shows the command output when there is not explicit-null label shimming:

```
Router# trace mpls ipv4 10.131.159.252/32
```

Tracing MPLS Label Switched Path to 10.131.159.252/32, timeout is 2 seconds

```
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'L' - labeled output interface, 'B' - unlabeled output interface,
'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
'M' - malformed request, 'm' - unsupported tlvs, 'N' - no rx label,
'P' - no rx intf label prot, 'p' - premature termination of LSP,
'R' - transit router, 'X' - unknown return code, 'x' - return code 0
```

Type escape sequence to abort.

```
0 10.131.191.252 MRU 1496 [Labels: 16/18 Exp: 0/0]
L 1 10.131.191.229 MRU 1508 [Labels: 18 Exp: 0] 4 ms
L 2 10.131.159.225 MRU 1504 [Labels: implicit-null Exp: 0] 4 ms
! 3 10.131.159.234 4 ms
```

## Viewing the AToM VCCV Capabilities Advertised to and Received from the Peer: Example

The following example shows that router PE1 advertises both AToM VCCV Type 1 and Type 2 switching capabilities and that the remote router PE2 advertises only a Type 2 switching capability.

```
Router# show mpls l2transport binding
```

```
Destination Address: 10.131.191.252, VC ID: 333
Local Label: 16
  Cbit: 1, VC Type: Ethernet, GroupID: 0
  MTU: 1500, Interface Desc: n/a
  VCCV Capabilities: Type 1, Type 2 <----- Locally advertised VCCV capabilities
Remote Label: 19
  Cbit: 1, VC Type: Ethernet, GroupID: 0
  MTU: 1500, Interface Desc: n/a
  VCCV Capabilities: Type 2 <-----Remotely advertised VCCV capabilities
```

## Additional References

The following sections provide references related to the MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature.

## Related Documents

Related Topic	Document Title
Usage examples for the IP ping and IP traceroute commands	<a href="#">Understanding the Ping and Traceroute Commands</a>
Configuration and verification tasks for MPLS LDP	<a href="#">MPLS Label Distribution Protocol (LDP) Overview</a>
Configuration and verification tasks for AToM	<a href="#">Any Transport over MPLS</a>
Switching services commands	<a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>
Automatic detection of which PE routers are added to or removed from the Virtual Private LAN Service (VPLS) domain	<a href="#">Information About VPLS Autodiscovery: BGP Based</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator, found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
draft-ietf-pwe3-vccv-01.txt	<a href="#">Pseudo-Wire (PW) Virtual Circuit Connection Verification (VCCV)</a>
RFC 2113	<a href="#">IP Router Alert Option</a>
RFC 4379	<a href="#">Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup>.

- **debug mpls lspv**
- **echo**
- **mpls oam**
- **ping mpls**
- **show mpls oam echo statistics**
- **trace mpls**



## Feature Information for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV

Table 7 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.0(27)S or Cisco IOS Release 12.4(6)T or 12.3(33)SXI or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 7 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 7** *Feature Information for MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV*

Feature Name	Releases	Feature Information
MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV	12.0(27)S 12.2(18)SXE 12.4(6)T 12.2(28)SB 12.0(32)SY 12.4(11)T 12.2(31)SB2 12.2(33)SRB 12.2(33)SXH 12.3(33)SXI	<p>The MPLS LSP Ping/Traceroute for LDP/TE, and LSP Ping for VCCV feature helps service providers monitor label switched paths and quickly isolate MPLS forwarding problems.</p> <p>In Cisco IOS Release 12.0(27)S, this feature was introduced. The following commands were introduced: <b>ping mpls</b> and <b>trace mpls</b>.</p> <p>The feature was incorporated into Cisco IOS Release 12.2(18)SXE. The following commands were modified: <b>ping mpls</b> and <b>trace mpls</b>.</p> <p>In Cisco IOS Release 12.4(6)T, the <b>mpls oam</b> command was introduced and the <b>trace mpls</b> command was modified.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB.</p> <p>The feature was incorporated into Cisco IOS Release 12.0(32)SY. The <b>show mpls oam echo statistics</b> command was added.</p> <p>The feature was incorporated into Cisco IOS Release 12.4(11)T. AToM Virtual Circuit Connection Verification (VCCV) is supported. The following commands were modified: <b>mpls oam</b>, <b>ping mpls</b>, and <b>trace mpls</b>.</p> <p>The feature was incorporated into Cisco IOS Release 12.2(31)SB2.</p> <p>In Cisco IOS Release 12.2(33)SRB, support for FEC 129 was added.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXH.</p> <p>This feature was integrated into Cisco IOS Release 12.2(33)SXI.</p>

# Glossary

**FEC**—forwarding equivalence class. A set of packets that can be handled equivalently for forwarding purposes and are thus suitable for binding to a single label. Examples include the set of packets destined for one address prefix and the packets in any flow.

**flow**—A set of packets traveling between a pair of hosts, or between a pair of transport protocol ports on a pair of hosts. For example, packets with the same source address, source port, destination address, and destination port might be considered a flow.

A flow is also a stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

**fragmentation**—The process of breaking a packet into smaller units when they are to be transmitted over a network medium that cannot support the original size of the packet.

**ICMP**—Internet Control Message Protocol. A network layer Internet protocol that reports errors and provides other information relevant to IP packet processing. It is documented in RFC 792.

**LFIB**—Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

**localhost**—A name that represents the host router (device). The localhost uses the reserved loopback IP address 127.0.0.1.

**LSP**—label switched path. A connection between two routers in which MPLS forwards the packets.

**LSPV**—Label Switched Path Verification. An LSP Ping subprocess. It encodes and decodes MPLS echo requests and replies, and it interfaces with IP, MPLS, and AToM switching for sending and receiving MPLS echo requests and replies. At the MPLS echo request originator router, LSPV maintains a database of outstanding echo requests for which echo responses have not been received.

**MPLS router alert label**—An MPLS label of 1. An MPLS packet with a router alert label is redirected by the router to the Route Processor (RP) processing level for handling. This allows these packets to bypass any forwarding failures in hardware routing tables.

**MRU**—maximum receive unit. Maximum size, in bytes, of a labeled packet that can be forwarded through an LSP.

**MTU**—maximum transmission unit. Maximum packet size, in bytes, that a particular interface can send or receive.

**punt**—Redirect packets with a router alert from the line card or interface to Route Processor (RP) level processing for handling.

**PW**—pseudowire. A form of tunnel that carries the essential elements of an emulated circuit from one provider edge (PE) router to another PE router over a packet-switched network.

**RP**—Route Processor. The processor module in a Cisco 7000 series router that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a supervisory processor.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. RSVP depends on IPv6. It is also known as Resource Reservation Setup Protocol.

**TLV**—type, length, values. A block of information included in a Cisco Discovery Protocol address.

**TTL hiding**—Time-to-live is a parameter you can set that indicates the maximum number of hops a packet should take to reach its destination.

**UDP**—User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, so error processing and retransmission must be handled by other protocols. UDP is defined in RFC 768.

---

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0908R)

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.





# MPLS EM - TE MIB RFC 3812

---

**First Published: November 20, 2009**

**Last Updated: November 20, 2009**

The MPLS EM - TE MIB RFC 3812 enables Simple Network Management Protocol (SNMP) agent support in Cisco IOS software for Multiprotocol Label Switching (MPLS) traffic engineering (TE) management, as implemented in the MPLS Traffic Engineering Standard MIB (MPLS TE STD MIB). The SNMP agent code operating in conjunction with the MPLS TE STD MIB enables a standardized, SNMP-based approach to be used in managing the MPLS TE features in Cisco IOS software.

The MPLS EM - TE MIB RFC 3812 feature introduces the MPLS-TE-STD-MIB, which is an upgrade from draft Version 6 of the MPLS-TE-MIB to an implementation of the *Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)*, RFC 3812.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for the MPLS EM - TE MIB RFC 3812](#)” section on page 16.

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

## Contents

- [Restrictions for the MPLS EM - TE MIB RFC 3812, page 2](#)
- [Information About the MPLS EM - TE MIB RFC 3812, page 2](#)
- [How to Configure the MPLS EM - TE MIB RFC 3812, page 11](#)
- [Configuration Examples for the MPLS EM - TE MIB RFC 3812, page 13](#)
- [Additional References, page 14](#)



---

**Americas Headquarters:**

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

- [Feature Information for the MPLS EM - TE MIB RFC 3812, page 16](#)
- [Glossary, page 17](#)

## Restrictions for the MPLS EM - TE MIB RFC 3812

The following restrictions apply to the MPLS TE STD MIB for Cisco IOS releases:

- Supports read-only (RO) permission for MIB objects.
- Contains no configuration support by means of SET functions, except for the `mplsTunnelTrapEnable` object (which has been made writable). Accordingly, the MPLS TE STD MIB contains indexing support for the Interfaces MIB.
- Supports only SNMP GET, GETNEXT, and GETBULK retrieval functions, except in the case of the `mplsTunnelTrapEnable` object (which has been made writable by means of SET functions).
- Contains no support for Guaranteed Bandwidth Traffic Engineering (GBTE) or Auto Bandwidth features.
- The following objects are not supported in Cisco IOS Release 12.2(33)SRE:

## Information About the MPLS EM - TE MIB RFC 3812

This section describes the following:

- [MPLS Traffic Engineering MIB Cisco Implementation, page 2](#)
- [Capabilities Supported by the MPLS EM TE MIB RFC 3812, page 3](#)
- [Notification Generation Events, page 3](#)
- [Notification Implementation, page 4](#)
- [Benefits of MPLS EM - TE MIB RFC 3812, page 4](#)
- [MPLS Traffic Engineering MIB Layer Structure, page 4](#)
- [Features and Technologies Related to MPLS EM - TE MIB RFC 3812, page 5](#)
- [Supported Objects in the MPLS EM - TE MIB RFC 3812, page 5](#)
- [CLI Access to MPLS EM - TE MIB RFC 3812 Information, page 9](#)

## MPLS Traffic Engineering MIB Cisco Implementation

The MPLS TE MIB is based on the Internet Engineering Task Force (IETF) draft MIB entitled *draft-ietf-mpls-te-mib-05.txt* which includes objects describing features that support MPLS TE.

Slight differences between the IETF draft MIB and the implementation of the TE capabilities within Cisco IOS software require some minor translations between the MPLS TE STD MIB and the internal data structures of Cisco IOS software. These translations are made by the SNMP agent code that is installed and operating on various hosts within the network. This SNMP agent code, running in the background as a low priority process, provides a management interface to Cisco IOS software.

The SNMP objects defined in the MPLS TE STD MIB can be displayed by any standard SNMP utility. All MPLS TE STD MIB objects are based on the IETF draft MIB; thus, no specific Cisco SNMP application is required to support the functions and operations pertaining to the MPLS TE STD MIB.

## MPLS Traffic Engineering Overview

MPLS TE capabilities in Cisco IOS software enable an MPLS backbone to replicate and expand upon the TE capabilities of Layer 2 ATM and Frame Relay networks.

TE capabilities are essential to effective management of service provider and Internet service provider (ISP) backbones. Such backbones must support high transmission capacities, and the networks incorporating backbones must be extremely resilient to link or node failures.

The MPLS TE facilities built into Cisco IOS software provide a feature-rich, integrated approach to managing the large volumes of traffic that typically flow through WANs. The MPLS TE facilities are integrated into Layer 3 network services, thereby optimizing the routing of IP traffic in the face of constraints imposed by existing backbone transmission capacities and network topologies.

## Capabilities Supported by the MPLS EM TE MIB RFC 3812

The following functionality is supported in the MPLS EM TE MIB RFC 3812:

- The ability to generate and queue notification messages that signal changes in the operational status of MPLS TE tunnels.
- Extensions to existing SNMP commands that provide the ability to enable, disable, and configure notification messages for MPLS TE tunnels.
- The ability to specify the name or the IP address of a network management station (NMS) in the operating environment to which notification messages are to be sent.
- The ability to write notification configurations into nonvolatile memory.

## Notification Generation Events

When MPLS TE notifications are enabled (see the **snmp-server enable traps mpls traffic-eng** command), notification messages relating to specific events within Cisco IOS software are generated and sent to a specified NMS in the network.

For example, an `mplsTunnelUp` notification is sent to an NMS when an MPLS TE tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.

Conversely, an `mplsTunnelDown` notification is generated and sent to an NMS when an MPLS TE tunnel transitions from an operationally “up” state to a “down” state.

An `mplsTunnelRerouted` notification is sent to the NMS when the signaling path of an existing MPLS TE tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).

An `mplsTunnelReoptimized` notification is sent when the signaling path of an existing MPLS TE tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by:

- A timer
- The issuance of an **mpls traffic-eng reoptimize** command
- A configuration change that requires the resignaling of a tunnel



Path options are configurable parameters that you can use to specify the order of priority for establishing a new tunnel path. For example, you can create a tunnel head configuration and define any one of many path options numbered 1 through  $n$ , with “1” being the highest priority option and “ $n$ ” being an unlimited number of lower priority path options. Thus, there is no limit to the number of path options that you can specify in this manner.

## Notification Implementation

When an MPLS TE tunnel interface (or any other device interface, such as an Ethernet or Packet over SONET (POS) interface) transitions between an up and down state, an Interfaces MIB (ifMIB) link notification is generated. When such a notification occurs in an MPLS TE STD MIB environment, the interface is checked by software to determine if the notification is associated with an MPLS TE tunnel. If so, the interfaces MIB link notification is interlinked with the appropriate `mplsTunnelUp` or `mplsTunnelDown` notification to provide notification to the NMS regarding the operational event occurring on the tunnel interface. Hence, the generation of an Interfaces MIB link notification pertaining to an MPLS traffic engineering tunnel interface begets an appropriate `mplsTunnelUp` or `mplsTunnelDown` notification that is transmitted to the specified NMS.

An `mplsTunnelRerouted` notification is generated whenever the signaling path for an MPLS TE tunnel changes. However, software intelligence in the MPLS TE STD MIB prevents the reroute notification from being sent to the NMS when a TE tunnel transitions between an up or down state during an administrative or operational status check of the tunnel. Either an up or down notification or a reroute notification can be sent in this instance, but not both. This action prevents unnecessary traffic on the network.

## Benefits of MPLS EM - TE MIB RFC 3812

The MPLS Traffic Engineering MIB provides the following benefits:

- Provides a standards-based SNMP interface for retrieving information about MPLS TE.
- Provides information about the traffic flows on MPLS TE tunnels.
- Presents MPLS TE tunnel routes, including the configured route, the Interior Gateway Protocol (IGP) calculated route, and the actual route traversed.
- Provides information, in conjunction with the Interfaces MIB, about how a tunnel was rerouted in the event of a link failure.
- Provides information about the configured resources used for an MPLS TE tunnel.
- Supports the generation and queueing of notifications that call attention to major changes in the operational status of MPLS TE tunnels;
- Forwards notification messages to a designated NMS for evaluation or action by network administrators.

## MPLS Traffic Engineering MIB Layer Structure

The SNMP agent code supporting the MPLS TE STD MIB follows the existing model for such code in Cisco IOS software and is, in part, generated by the Cisco IOS tool set, based on the MIB source code.

The SNMP agent code, which has a layered structure similar to that of the MIB support code in Cisco IOS software, consists of four layers:

- Platform independent layer—This layer is generated primarily by the Cisco IOS MIB development tool set and incorporates platform and implementation independent functions. The Cisco IOS MIB development tool set creates a standard set of files associated with a MIB.
- Application interface layer—The functions, names, and template code for MIB objects in this layer are also generated by the Cisco IOS MIB development tool set.
- Application specific layer—This layer provides an interface between the application interface layer and the application program interface (API) and data structures layer and performs tasks needed to retrieve required information from Cisco IOS software, such as searching through data structures.
- API and data structures layer—This layer contains the data structures or APIs within Cisco IOS software that are retrieved or called in order to set or retrieve SNMP management information.

## Features and Technologies Related to MPLS EM - TE MIB RFC 3812

The MPLS TE STD MIB feature is used in conjunction with the following features and technologies:

- Standards-based SNMP network management application
- MPLS
- MPLS TE
- MPLS label switching router MIB (MPLS-LSR-MIB)

## Supported Objects in the MPLS EM - TE MIB RFC 3812

The MPLS TE STD MIB contains numerous tables and object definitions that provide read-only SNMP management support for the MPLS TE features in Cisco IOS software. The MPLS TE STD MIB conforms to Abstract Syntax Notation One (ASN.1), thus reflecting an idealized MPLS TE database.

Using any standard SNMP network management application, you can retrieve and display information from the MPLS TE STD MIB by using GET operations; similarly, you can traverse information in the MIB database for display by using GETNEXT operations.

The MPLS TE STD MIB tables and objects supported in Cisco IOS releases follow. Important MIB tables (those highlighted in bold type) are described briefly in accompanying text.

- **mplsTunnelConfigured**—Total number of tunnel configurations that are defined on this node.
- **mplsTunnelActive**—Total number of label switched paths (LSPs) that are defined on this node.
- **mplsTunnelTEDistProto**—The IGP distribution protocol in use.
- **mplsTunnelMaxHops**—The maximum number of hops any given tunnel can utilize.
- **mplsTunnelIndexNext**—Unsupported; set to 0.
- **mplsTunnelTable**—Entries in this table with an instance of 0 and a source address of 0 represent tunnel head configurations. All other entries in this table represent instances of LSPs, both signaled and standby. If a tunnel instance is signaled, its operating status (operStatus) is set to “up” (1) and its instance corresponds to an active LSP.

Tunnel configurations exist only on the tunnel head where the tunnel interface is defined. LSPs traverse the network and involve tunnel heads, tunnel midpoints, and tunnel tails.

Pointers in the tunnel table refer to corresponding entries in other MIB tables. By using these pointers, you can find an entry in the `mplsTunnelTable` and follow a pointer to other tables for additional information. The pointers are the following: *mplsTunnelResourcePointer*, *mplsTunnelHopTableIndex*, *mplsTunnelARHopTableIndex*, and *mplsTunnelCHopTableIndex*.

The tunnel table is indexed by tunnel ID, tunnel instance, tunnel source address, and tunnel destination address. The description of each entry has an alphabetic suffix (a), (b), or (c), if appropriate, to indicate the applicability of the entry:

- a. For tunnel head configurations only
- b. For LSPs only
- c. For both tunnel head configurations and LSPs

Following is a list and description of each entry.

- `mplsTunnelIndex`—Same as tunnel ID (c).
- `mplsTunnelInstance`—Tunnel instance of the LSP; 0 for head configurations (b).
- `mplsTunnelIngressLSRId`—Source IP address of the LSP; 0 for head configurations (b).
- `mplsTunnelEgressLSRId`—Destination IP address of the tunnel (c).
- `mplsTunnelName`—Command name for the tunnel interfaces (a).
- `mplsTunnelDescr`—Descriptive name for tunnel configurations and LSPs (c).
- `mplsTunnelIsIf`—Indicator of whether the entry represents an interface (c).
- `mplsTunnelIfIndex`—Index of the tunnel interface within the `ifMIB` (a).
- `mplsTunnelXCPointer`—(For midpoints only – no tails) Pointer for the LSP within the `mplsXCTable` of the MPLS LSR STD MIB (b).
- `mplsTunnelSignallingProto`—Signaling protocol used by tunnels (c).
- `mplsTunnelSetupPrio`—Setup priority of the tunnel (c).
- `mplsTunnelHoldingPrio`—Holding priority of the tunnel (c).
- `mplsTunnelSessionAttributes`—Session attributes (c).
- `mplsTunnelOwner`—Tunnel owner (c).
- `mplsTunnelLocalProtectInUse`—Not implemented (c).
- `mplsTunnelResourcePointer`—Pointer into the Resource Table (b).
- `mplsTunnelInstancePriority`—Not implemented (b).
- `mplsTunnelHopTableIndex`—Index into the Hop Table (a).
- `mplsTunnelARHopTableIndex`—Index into the AR Hop Table (b).
- `mplsTunnelCHopTableIndex`—Index into the C Hop Table (b).
- `mplsTunnelPrimaryUpTime`—Amount of time, in seconds, that the current path has been up (a).
- `mplsTunnelPathChanges`—Number of times a tunnel has been resignalled (a).
- `mplsTunnelLastPathChange`—Amount of time, in seconds, since the last path resignaling occurred (a).
- `mplsTunnelCreationTime`—Time stamp when the tunnel was created (a).
- `mplsTunnelStateTransitions`—Number of times the tunnel has changed state (a).
- `mplsTunnelIncludeAnyAffinity`—Not implemented (a).

- `mplsTunnelIncludeAllAffinity`—Attribute bits that must be set for the tunnel to traverse a link (a).
- `mplsTunnelExcludeAnyAffinity`—Attribute bits that must *not* be set for the tunnel to traverse a link (a).
- `mplsTunnelPathInUse`—Path option number being used for the tunnel’s path. If no path option is active, this object will be 0 (a).
- `mplsTunnelRole`—Role of the tunnel on the router; that is, head, midpoint, or tail (c).
- `mplsTunnelTotalUpTime`—Amount of time, in seconds, that the tunnel has been operationally up (a).
- `mplsTunnelInstanceUpTime`—Not implemented (b).
- `mplsTunnelAdminStatus`—Administrative status of a tunnel (c).
- `mplsTunnelOperStatus`—Actual operating status of a tunnel (c).
- `mplsTunnelRowStatus`—This object is used in conjunction with configuring a new tunnel. This object will always be seen as “active” (a).
- `mplsTunnelStorageType`—Storage type of a tunnel entry (c).
- `mplsTunnelHopListIndexNext`—Next valid index to use as an index in the `mplsTunnelHopTable`.
- **`mplsTunnelHopTable`**—Entries in this table exist only for tunnel configurations and correspond to the path options defined for the tunnel. Two types of path options exist: *explicit* and *dynamic*. This table shows all hops listed in the explicit path options, while showing only the destination hop for dynamic path options. The tunnel hop table is indexed by tunnel ID, path option, and hop number.

Following is a list and description of each table entry.

- `mplsTunnelHopListIndex`—Primary index into the table.
- `mplsTunnelHopIndex`—Secondary index into the table.
- `mplsTunnelHopAddrType`—Indicates if the address of this hop is the type IPv4 or IPv6.
- `mplsTunnelHopIpAddr`—The IP address of this hop.
- `mplsTunnelHopIpPrefixLen`—The prefix length of the IP address.
- `mplsTunnelHopAsNumber`—This object will contain 0 or the autonomous system number of the hop, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopLspId`—This object will contain 0 or the LSPID of the tunnel, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelHopType`—Denotes whether this tunnel hop is routed in a strict or loose fashion.
- `mplsTunnelHopInclude`—Indicates whether this hop must be included in the tunnel.
- `mplsTunnelHopPathOptionName`—Describes a series of hops as they relate to a specified path option.
- `mplsTunnelHopEntryPathComp`—Indicates whether the complete tunnel path should be specified.
- `mplsTunnelHopRowStatus`—This object is used in conjunction with the configuring of a new row in the table.
- `mplsTunnelHopStorageType`—The storage type of this MIB object.
- `mplsTunnelResourceIndexNext`—This object contains the next appropriate value to be used for `mplsTunnelResourceIndex` when creating entries in the `mplsTunnelResourceTable`

- **mplsTunnelResourceTable**—Entries in this table correspond to the “Tspec” information displayed when you execute the **show mpls traffic-eng tunnels** command. These entries exist only for LSPs.

The tunnel resource table is indexed by address and hop number. Following the *mplsTunnelResourcePointer* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry.

- *mplsTunnelResourceIndex*—The primary index into this table.
- *mplsTunnelResourceMaxRate*—The maximum rate, in bits per second, supported by this tunnel.
- *mplsTunnelResourceMeanRate*—The mean rate, in bits per second, supported by this tunnel.
- *mplsTunnelResourceMaxBurstSize*—The maximum burst size, in bytes, allowed by this tunnel.
- *mplsTunnelResourceRowStatus*—This object is used in conjunction with the configuration of a new row in the table.
- *mplsTunnelResourceStorageType*—The storage type of this MIB object.
- **mplsTunnelARHopTable**—Entries in this table correspond to the actual route taken by the tunnel, and whose route was successfully signaled by the network. The hops present in this table correspond to those present in the record route object (RRO) in Resource Reservation Protocol (RSVP). You can also display the information in this table by executing the **show mpls traffic-eng tunnels** command.

The actual route hop table is indexed by address and hop number. Following the *mplsTunnelARHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry:

- *mplsTunnelARHopListIndex*—The primary index into this table.
- *mplsTunnelARHopIndex*—The secondary index into this table.
- *mplsTunnelARHopIpAddr*—The IP address of this hop.
- *mplsTunnelARHopIpPrefixLen*—The prefix length of the IP address.
- *mplsTunnelARHopAsNumber*—This object will contain 0 or the AS number of the hop, depending on the value of *mplsTunnelARHopAddrType*.
- *mplsTunnelARHopAddrType*—The type of address for this MIB entry, either IPv4 or IPv6.
- *mplsTunnelARHopType*—Denotes whether this tunnel hop is routed in a strict or loose manner.
- **mplsTunnelCHopTable**—Entries in this table correspond to the explicit route object (ERO) in RSVP, which is used to signal the LSP. The list of hops in this table will contain those hops that are computed by the constraint-based shortest path first (SPF) algorithm. In those cases where “loose” hops are specified for the tunnel, this table will contain the hops that are “filled-in” between the loose hops to complete the path. If you specify a complete explicit path, the computed hop table matches your specified path.

The computed hop table is indexed by address and hop number. Following the *mplsTunnelCHopTableIndex* pointer from the tunnel table is the best way to retrieve information from this table.

Following is a list and description of each table entry:

- *mplsTunnelCHopListIndex*—The primary index into this table.
- *mplsTunnelCHopIndex*—The secondary index into this table.
- *mplsTunnelCHopAddrType*—Indicates if the address of this hop is the type IPv4 or IPv6.

- `mplsTunnelCHopIpAddr`—The IP address of this hop.
- `mplsTunnelCHopIpPrefixLen`—The prefix length of the IP address.
- `mplsTunnelCHopAsNumber`—This object will contain 0 or the autonomous system number of the hop, depending on the value of `mplsTunnelHopAddrType`.
- `mplsTunnelCHopType`—Denotes whether this tunnel hop is routed in a strict or loose way.
- **`mplsTunnelPerfTable`**—The tunnel performance table, which augments the **`mplsTunnelTable`**, provides packet and byte counters for each tunnel. This table contains the following packet and byte counters:
  - `mplsTunnelPerfPackets`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfHCPackets`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfErrors`—This packet counter works only for tunnel heads.
  - `mplsTunnelPerfBytes`—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.
  - `mplsTunnelPerfHCBytes`—This byte counter works for tunnel heads and tunnel midpoints, but not for tunnel tails.
- `mplsTunnelTrapEnable`—The object type *`mplsTunnelTrapEnable`* is enhanced to be writable. Accordingly, if this object type is set to “TRUE,” the following notifications are enabled, thus giving you the ability to monitor changes in the operational status of MPLS TE tunnels:
  - `mplsTunnelUp`
  - `mplsTunnelDown`
  - `mplsTunnelRerouted`
  - `mplsTunnelReoptimized`

If the *`mplsTunnelTrapEnable`* object is set to “FALSE,” such operational status notifications are not generated. These notification functions are based on the definitions (`mplsTeNotifications`) contained in the IETF draft document entitled *`draft-ietf-mpls-te-mib-05.txt`*.

## CLI Access to MPLS EM - TE MIB RFC 3812 Information

Figure 1 shows commands that you can use to retrieve information from specific tables in the MPLS TE MIB. As noted in this figure, some information in the MPLS TE STD MIB is not retrievable by commands.

**Figure 1**      **Commands for Retrieving MPLS TE STD MIB Information**

		show mpls traffic-eng tunnels	show mpls traffic-eng tunnels summary	show ip explicit-paths	show interfaces	Not available in command
mplsTunnelTable	x				x	
mplsTunnelHopTable	x		x			
mplsTunnelResourceTable	x					
mplsTunnelARHopTable	x					
mplsTunnelCHopTable	x					
mplsTunnelPerfTable	x			x		
Scalars	x	x			x	

52510

## Retrieving Information from the MPLS EM - TE MIB RFC 3812

This section describes how to efficiently retrieve information about TE tunnels. Such information can be useful in large networks that contain many TE tunnels.

Traverse across a single column of the *mplsTunnelTable*, such as *mplsTunnelName*. This action provides the indexes of every tunnel configuration, and any LSPs involving the host router. Using these indexes, you can perform a GET operation to retrieve information from any column and row of the *mplsTunnelTable*.

The *mplsTunnelTable* provides pointers to other tables for each tunnel. The column *mplsTunnelResourcePointer*, for example, provides an object ID (OID) that you can use to access resource allocation information in the *mplsTunnelResourceTable*. The columns *mplsTunnelHopTableIndex*, *mplsTunnelARHopTableIndex*, and *mplsTunnelCHopTableIndex* provide the primary index into the *mplsTunnelHopTable*, *mplsTunnelARHopTable*, and *mplsTunnelCHopTable*, respectively. By traversing the MPLS TE STD MIB in this manner using a hop table column and primary index, you can retrieve information pertaining to the hops of that tunnel configuration.

Because tunnels are treated as interfaces, the tunnel table column (*mplsTunnelIfIndex*) provides an index into the Interfaces MIB that you can use to retrieve interface-specific information about a tunnel.

# How to Configure the MPLS EM - TE MIB RFC 3812

This section contains the following tasks:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router, page 11](#) (required)
- [Verifying the Status of the SNMP Agent, page 12](#) (optional)

## Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router

The SNMP agent for the MPLS TE STD MIB is disabled by default. To enable the SNMP agent for the MPLS TE STD MIB, perform the following steps.

### SUMMARY STEPS

1. `telnet host`
2. `enable`
3. `show running-config`
4. `configure terminal`
5. `snmp-server community string [view view-name] [ro | rw] [ipv6 nacl] [access-list-number]`
6. `snmp-server enable traps [identification-type] [notification-option]`
7. `exit`
8. `write memory`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>telnet host</code>  <b>Example:</b> Router> telnet 192.172.172.172	Telnets to the router identified by the specified IP address (represented as xxx.xxx.xxx.xxx).
Step 2	<code>enable</code>  <b>Example:</b> Router# enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 3	<code>show running-config</code>  <b>Example:</b> Router# show running-config	Displays the running configuration to determine if an SNMP agent is already running. <ul style="list-style-type: none"><li>• If no SNMP information is displayed, go to <a href="#">Step 4</a>. If any SNMP information is displayed, you can modify the information or change it as needed.</li></ul>



	Command or Action	Purpose
Step 4	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 5	<code>snmp-server community string [view view-name] [ro   rw] [ipv6 nacl] [access-list-number]</code>  <b>Example:</b> Router(config)# <code>snmp-server community comaccess ro 4</code>	Enables the read-only (RO) community string.
Step 6	<code>snmp-server enable traps [identification-type] [notification-option]</code>  <b>Example:</b> Router(config)# <code>snmp-server enable traps</code>	Enables an LSR to send SNMP notifications or informs to an SNMP host.  <b>Note</b> This command is optional. After SNMP is enabled, all MIBs (not just the TE MIB) are available for the user to query.
Step 7	<code>exit</code>  <b>Example:</b> Router(config)# <code>exit</code>	Exits global configuration mode and returns to privileged EXEC mode.
Step 8	<code>write memory</code>  <b>Example:</b> Router# <code>write memory</code>	Writes the modified configuration to NVRAM, permanently saving the settings.

## Verifying the Status of the SNMP Agent

To verify that the SNMP agent has been enabled on a host network device, perform the following steps.

### SUMMARY STEPS

1. `telnet host`
2. `enable`
3. `show running-config`

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>telnet</b> <i>host</i>  <b>Example:</b> Router# telnet 192.172.172.172	Telnet to the target device identified by the specified IP address (represented as <i>xxx.xxx.xxx.xxx</i> ).
Step 2	<b>enable</b>  <b>Example:</b> Router# enable	Enables SNMP on the target device.
Step 3	<b>show running-config</b>  <b>Example:</b> Router# show running-config	Displays the running configuration on the target device and is used to examine the output for displayed SNMP information.

## Examples

The following example displays the running configuration on the target device and its SNMP information.

```
Router# show running-config
.
.
.
snmp-server community public ro
snmp-server community private ro
```

Any **snmp-server** statement that appears in the output and takes the form shown here verifies that SNMP has been enabled on that device.

# Configuration Examples for the MPLS EM - TE MIB RFC 3812

This section contains the following configuration examples:

- [Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example, page 13](#)

## Enabling the SNMP Agent to Help Manage Various MPLS TE Tunnel Characteristics of Tunnels on the Local Router: Example

The following example shows how to enable an SNMP agent on a host network device:

```
Router# configure terminal
Router(config)# snmp-server community private
```

The following example shows how to enable SNMPv1 and SNMPv2C. The configuration permits any SNMP agent to access all MPLS TE STD MIB objects with read-only permissions using the community string *public*.

```
Router(config)# snmp-server community public
```

The following example shows how to allow read-only access to all MPLS TE STD MIB objects relating to members of access list 4 that specify the *comaccess* community string. No other SNMP agents will have access to any MPLS TE STD MIB objects.

```
Router(config)# snmp-server community comaccess ro 4
```

## Additional References

The following sections provide references related to the MPLS EM - TE MIB RFC 3812.

### Related Documents

Related Topic	Document Title
MPLS-based functionalities	<ul style="list-style-type: none"> <li><i>MPLS Label Distribution Protocol (LDP)</i></li> <li><i>MPLS Label Switching Router MIB</i></li> <li><i>MPLS Scalability Enhancements for the LSC LSR</i></li> <li><i>MPLS Scalability Enhancements for the ATM LSR</i></li> <li><i>MPLS Traffic Engineering (TE)—Automatic Bandwidth Adjustment for MPLS TE Tunnels</i></li> <li><i>MPLS Traffic Engineering (TE)—Scalability Enhancements</i></li> <li><i>MPLS Class of Service Enhancements</i></li> <li><i>RFC 2233 Interfaces MIB</i></li> </ul>

### Standards

Standard	Title
draft-ietf-mpls-te-mib-05	MPLS Traffic Engineering Management Information Base Using SMIv2

### MIBs

MIB	MIBs Link
MPLS TE MIB Interfaces MIB MPLS TE STD MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 2026	<i>The Internet Standards Process</i>
RFC 3812	<i>Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB)</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for the MPLS EM - TE MIB RFC 3812

Table 1 lists the release history for this MIB.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for the MPLS EM - TE MIB RFC 3812

Feature Name	Releases	Feature Information
MPLS-EN TE MIB RFC 3812	12.2(33)SRE	<p>The MPLS EM - TE MIB RFC 3812 feature enables the SNMP agent support in Cisco IOS software for MPLS TE management, as implemented in the MPLS TE STD MIB.</p> <p>The following commands were introduced or modified:  <b>snmp-server community</b>, <b>snmp-server enable traps mpls rfc</b>, <b>snmp-server enable traps mpls traffic-eng</b>, <b>snmp-server host</b>.</p>

# Glossary

**affinity bits**—An MPLS traffic engineering tunnel’s requirements on the attributes of the links it will cross. The tunnel’s affinity bits and affinity mask must match with the attributes of the various links carrying the tunnel.

**call admission precedence**—An MPLS traffic engineering tunnel with a higher priority will, if necessary, preempt an MPLS traffic engineering tunnel with a lower priority. An expected use is that tunnels that are more difficult to route will have a higher priority, and can preempt tunnels that are less difficult to route, on the assumption that those lower priority tunnels can find another path.

**constraint-based routing**—Procedures and protocols used to determine a route across a backbone taking into account resource requirements and resource availability, instead of simply using the shortest path.

**flow**—A traffic load entering the backbone at one point—point of presence (POP)—and leaving it from another that must be traffic engineered across the backbone. The traffic load will be carried across one or more LSP tunnels running from the entry POP to the exit POP.

**headend**—The LSR at which the tunnel originates. The tunnel’s “head” or tunnel interface will reside at this LSR as well.

**informs**—A type of notification message that is more reliable than a conventional trap notification message because an informs message requires acknowledgment.

**label**—A short, fixed-length data construct that tells switching nodes how to forward data (packets or cells).

**label switched path (LSP) tunnel**—A configured connection between two routers, using label switching to carry the packets.

**LSP**—label switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

**LSR**—label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MIB**—Management Information Base. A database of network management information (consisting of MIB objects) that is used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands, usually by a GUI-based network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

**MPLS**—Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**NMS**—network management station. An NMS is a powerful, well-equipped computer (typically an engineering workstation) that is used by a network administrator to communicate with other devices in the network. An NMS is typically used to manage network resources, gather statistics, and perform a variety of network administration and configuration tasks.

**notification**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred (see traps).

**OSPF**—Open Shortest Path First. A link-state routing protocol used for routing IP.

**RSVP**—Resource Reservation Protocol. Protocol for reserving network resources to provide quality of service (QoS) guarantees to application flows.

**SNMP**—Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, manage configurations, collect statistics, monitor performance, and ensure network security.

**tailend**—The downstream, receive end of a tunnel.

**traffic engineering**—Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

**trap**—A message sent by an SNMP agent to a network management station, console, or terminal to indicate that a significant event within Cisco IOS software has occurred. Traps (notifications) are less reliable than inform requests, because the receiver of the trap does not send an acknowledgment of receipt; furthermore, the sender of the trap cannot determine if the trap was received (see notification).

**VCC**—virtual channel connection. A VCC is a logical circuit consisting of VCLs that carries data between two endpoints in an ATM network. Sometimes called a virtual circuit connection.

**VCI**—virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next network VCL as the cell passes through a series of ATM switches on its way to its final destination.

**VCL**—virtual channel link. A VCL is the logical connection that exists between two adjacent switches in an ATM network.

**VPI**—virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next network VCL as the cell passes through a series of ATM switches on its way to its final destination.

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

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

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

© 2001–2009 Cisco Systems, Inc. All rights reserved.



## **MPLS High Availability**







# MPLS High Availability: Overview

---

**First Published: August 11, 2004**

**Last Updated: August 21, 2007**

This document provides an overview of the Multiprotocol Label Switching (MPLS) high availability (HA) features. MPLS HA provides full nonstop forwarding (NSF) and stateful switchover (SSO) capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Networks (VPNs) features.

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS High Availability: Overview”](#) section on page 9.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Restrictions for MPLS High Availability](#)
- [Information About MPLS High Availability, page 2](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Feature Information for MPLS High Availability: Overview, page 9](#)



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Restrictions for MPLS High Availability

For information about supported hardware, see the following documents:

- For Cisco IOS Release 12.2(25)S, see the [Cross-Platform Release Notes for Cisco IOS Release 12.2S](#).
- For Cisco IOS Release 12.2SB, see the [Cross-Platform Release Notes for Cisco IOS Release 12.2SB](#).
- For Cisco IOS Release 12.2(33)SRA, see the [Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers](#)
- For Cisco IOS Release 12.2(33)SXH, see the [Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 Series MSFC](#)

## Information About MPLS High Availability

This section covers the following topics:

- [MPLS High Availability Overview, page 2](#)
- [MPLS High Availability Features, page 3](#)
- [MPLS High Availability Infrastructure Changes, page 4](#)
- [MPLS Applications That Coexist with SSO, page 5](#)

## MPLS High Availability Overview

MPLS HA features provide SSO and NSF capability to the MPLS Label Distribution Protocol (LDP) and MPLS Virtual Private Network (VPN) features. MPLS HA includes the following new features:

- [NSF/SSO—MPLS VPN](#)
- [NSF/SSO—MPLS LDP and LDP Graceful Restart](#)
- [NSF/SSO: Any Transport over MPLS and Graceful Restart](#)

In addition, the MIBs for MPLS VPNs and MPLS LDP have been enhanced to work in the MPLS HA environment.

The following features have been changed or created to work in the MPLS HA environment:

- [MPLS High Availability Infrastructure Changes](#)
- [Cisco Express Forwarding Scalability Enhancements](#)

The following features perform normally in an NSF/SSO environment. They can exist with SSO and NSF but do not have the ability to keep duplicate information in a backup Route Processor (RP) on the Cisco 7500 series router and in a backup Performance Routing Engine2 (PRE2) on the Cisco 10000 series router.

- [MPLS Traffic Engineering](#)
- [MPLS Quality of Service Applications](#)
- [IPv6 over MPLS](#) (not supported on the Cisco 10000 series router)
- [MPLS Label Switching Router MIB](#)
- [MPLS TE MIB](#)

- [MPLS Enhancements to Interfaces MIB](#)

The following sections explain these features in more detail.

## MPLS High Availability Features

The following MPLS HA features have the ability to continue forwarding data following an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router:

- MPLS Label Distribution Protocol (LDP)
- MPLS Virtual Private Networks (VPNs)
- Any Transport over MPLS (AToM)

**Note**

In Cisco IOS Release 12.2(28)SB, AToM is not enabled for high availability on the Cisco 10000 series router. However, AToM coexists with SSO. This means that AToM functions normally in an SSO environment but because state information is not maintained on the standby RP, a switchover can partially disrupt operations

When you enable MPLS HA, you get the benefit of allowing an RP on the Cisco 7500 series router or PRE2 on the Cisco 10000 series router to recover from disruption in service without losing its LDP bindings, MPLS forwarding state, and VPN prefix information.

### NSF/SSO—MPLS VPN

The NSF/SSO—MPLS VPN feature allows a router to recover from a disruption in service without losing its VPN prefix information. The NSF/SSO—MPLS VPN feature works with the BGP Graceful Restart mechanisms defined in the Graceful Restart Internet Engineering Task Force (IETF) specifications and in the [Cisco Nonstop Forwarding](#) feature module. The BGP Graceful Restart feature supports the VPNv4 VRFs, which allows the routers running BGP Graceful Restart to preserve VPN prefix information when a router restarts.

For information about configuring the NSF/SSO—MPLS VPN feature, see the following feature module: [NSF/SSO—MPLS VPN](#).

### NSF/SSO: MPLS VPN MIB

The NSF/SSO—MPLS VPN feature works with the MPLS VPN MIB. For information about configuring the MPLS VPN MIB, see the following feature module: [MPLS VPN: SNMP MIB Support](#).

### NSF/SSO—MPLS LDP and LDP Graceful Restart

MPLS LDP uses SSO, NSF, and Graceful Restart to allow an RP on the Cisco 7500 series router or PRE2 on the Cisco 10000 series router to recover from disruption in the LDP components of the control plane service without losing its MPLS forwarding state. The NSF/SSO—MPLS LDP and LDP Graceful Restart feature works with LDP sessions between directly connected peers as well as with peers that are not directly connected (targeted sessions).

For information about configuring the NSF/SSO—MPLS LDP and LDP Graceful Restart feature, see the following feature module: [NSF/SSO—MPLS LDP and LDP Graceful Restart](#).

## NSF/SSO: MPLS LDP MIB

The MPLS LDP MIB with the IETF Version 8 Upgrade is supported with NSF/SSO—MPLS LDP and LDP Graceful Restart. For information about configuring the MPLS LDP MIB, see the following feature module: [MPLS Label Distribution Protocol MIB Version 8 Upgrade](#).

## NSF/SSO: Any Transport over MPLS and Graceful Restart

AToM uses SSO, NSF, and Graceful Restart to allow an RP to recover from disruption in the LDP components of the control plane service without losing its MPLS forwarding state.



### Note

In Cisco IOS Release 12.2(28)SB, AToM is not enabled for high availability on the Cisco 10000 series router. However, AToM coexists with SSO. This means that AToM functions normally in an SSO environment but because state information is not maintained on the standby RP, a switchover can partially disrupt operations.

For information about configuring AToM NSF/SSO Support and Graceful Restart, see [NSF/SSO: Any Transport over MPLS and Graceful Restart](#).

## MPLS High Availability Infrastructure Changes

The MPLS control plane software has been enhanced to work in an HA environment. The changes made the control plane software more modular, which helps MPLS support newer applications. Some of the control plane software changes made MPLS more scalable and flexible. See the [“Cisco Express Forwarding Scalability Enhancements”](#) section on page 4 for more information.

Changes to the MPLS Forwarding Infrastructure (MFI) and the Cisco Express Forwarding component introduced new commands and changed other existing commands.

MFI replaced the Label Forwarding Information Base (LFIB) and is responsible for managing MPLS data structures used for forwarding. For information about the MPLS command changes related to the MFI, see the following document: [MPLS High Availability: Command Changes](#).



### Note

The MFI and LFIB do not coexist in the same image. Users must use MFI starting with Cisco IOS Release 12.2(25)S and later releases.

MPLS High Availability introduces the MPLS IP Rewrite Manager (IPRM), which manages the interactions between Cisco Express Forwarding, the IP Label Distribution Modules (LDMs), and the MFI. MPLS IPRM is enabled by default. You do not need to configure or customize the IPRM. See the [“Command Reference”](#) section on page 8 for show and debug commands related to IPRM.

## Cisco Express Forwarding Scalability Enhancements

Cisco Express Forwarding provides a forwarding path and maintains a complete forwarding and adjacency table for both the software and hardware forwarding engines.

With MPLS High Availability, Cisco Express Forwarding supports new features and new hardware. The Cisco Express Forwarding improvements enable Cisco Express Forwarding to work with the MPLS HA applications and the MFI infrastructure. Cisco Express Forwarding improvements increase scalability, which are outlined in [Table 1](#).

**Table 1** Cisco Express Forwarding Scalability Enhancements

For the Cisco 7500 Series Router	For the Cisco 10000 Series Router
Up to 512,000 prefixes	Up to 1 million prefixes
Up to 128,000 adjacencies	Up to 1 million adjacencies
4000 VPNs	4000 VPNs
Arbitrary prefix path counts from the Routing Information Base (RIB)	Arbitrary prefix path counts from the RIB
16 paths per prefix for forwarding	8 paths per prefix for forwarding
64 Cisco Express Forwarding instances (such as line cards or redundant RPs)	NA

Cisco Express Forwarding makes the following enhancements:

- Improves memory use
- Reduces large peak memory use
- Reduces route convergence times for the Cisco 7500 series router.

For information about the Cisco Express Forwarding command changes, see [Cisco Express Forwarding: Command Changes](#).

## MPLS Applications That Coexist with SSO

The following sections list the MPLS features that maintain, either partially or completely, undisturbed operation through an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router.

### MPLS Traffic Engineering

The MPLS Traffic Engineering (TE) features work with the new Cisco Express Forwarding and MFI modules. TE is SSO coexistent, which means it maintains, either partially or completely, undisturbed operation through an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router. No additional capabilities have been introduced with MPLS High Availability. The **debug mpls traffic-eng lsd-client** command is introduced with the MPLS High Availability features.

### MPLS Quality of Service Applications

Cisco IOS MPLS supports the IETF DiffServ architecture by enabling the quality of service (QoS) functions listed in [Table 2](#) to act on the MPLS packets.

**Table 2** MPLS QoS Support

Category	Related MPLS QoS Features
Traffic classification	Access Control List matching
Traffic marking	Differentiated services code point (DSCP) MPLS Experimental (EXP) field

**Table 2**      **MPLS QoS Support (continued)**

Category	Related MPLS QoS Features
Congestion management	Low latency queueing (LLQ) Class-based weighted fair queueing (CBWFQ)
Congestion avoidance	Weighted Random Early Detection (WRED)
Traffic conditioning	Shaping and policing

## IPv6 over MPLS

The IPv6 over MPLS application works with the new Cisco Express Forwarding and MFI modules. IPv6 over MPLS is SSO coexistent, which means it maintains, either partially or completely, undisturbed operation through an RP switchover.



### Note

The Cisco 10000 series router does not support the IPv6 over MPLS application.

Command changes are documented in the [Cisco IOS IPv6 Command Reference](#).

## MPLS Label Switching Router MIB

The MPLS Label Switching Router (LSR) MIB works in the MPLS HA environment. Two indexes in the LSR MIB were changed to provide well-defined and ordered values:

- mplsXCIndex
- mplsOutSegmentIndex

This benefits the MPLS LSR MIB in the following ways:

- The MIB walk-through has a consistent and logical order.
- The same index values are maintained after a switchover.

For information about the MPLS LSR MIB, see the [MPLS Label Switching Router MIB](#).

## MPLS TE MIB

The MPLS TE MIB works in the MPLS HA environment. For information about the MPLS TE MIB, see the [MPLS Traffic Engineering \(TE\) MIB](#).



### Note

After an RP switchover on the Cisco 7500 series router or PRE2 switchover on the Cisco 10000 series router, the value of mplsTunnelCreationTime in the TE MIB does not correctly reflect the time when the tunnel was created. After an RP or PRE2 switchover, the tunnel gets a new time stamp.

## MPLS Enhancements to Interfaces MIB

The MPLS Enhancements to Interfaces MIB works in the MPLS HA environment. For information about the MPLS Enhancements to Interfaces MIB, see the [MPLS Enhancements to Interfaces MIB](#).

# Additional References

The following sections provide references related to the MPLS High Availability feature.

## Related Documents

Related Topic	Document Title
MPLS VPNs Non Stop Forwarding	<a href="#">NSF/SSO—MPLS VPN</a>
MPLS LDP Non Stop Forwarding	<a href="#">NSF/SSO—MPLS LDP and LDP Graceful Restart</a>
AToM Non Stop Forwarding	<a href="#">NSF/SSO: Any Transport over MPLS and Graceful Restart</a>
Cisco Express Forwarding	<a href="#">Cisco Express Forwarding: Command Changes</a>
MIBs	<ul style="list-style-type: none"> <li>• <a href="#">MPLS VPN: SNMP MIB Support</a></li> <li>• <a href="#">MPLS Label Distribution Protocol MIB Version 8 Upgrade</a></li> <li>• <a href="#">MPLS Label Switching Router MIB</a></li> <li>• <a href="#">MPLS Enhancements to Interfaces MIB.</a></li> <li>• <a href="#">MPLS Traffic Engineering (TE) MIB</a></li> </ul>
NSF/SSO	<a href="#">Cisco Nonstop Forwarding</a> <a href="#">MPLS High Availability: Command Changes</a>

## Standards

Standard	Title
draft-ietf-mpls-bgp-mpls-restart.txt	Graceful Restart Mechanism for BGP with MPLS
draft-ietf-mpls-idr-restart.txt	Graceful Restart Mechanism for BGP

## MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> <li>• MPLS VPN MIB</li> <li>• MPLS Label Distribution Protocol MIB Version 8 Upgrade</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 3478	Graceful Restart Mechanism for Label Distribution



## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **clear mpls counters**
- **clear mpls ip iprm counters**
- **debug mpls ip iprm**
- **debug mpls ip iprm cef**
- **debug mpls ip iprm events**
- **debug mpls ip iprm ldm**
- **debug mpls ip iprm mfi**
- **debug mpls traffic-eng lsd-client**
- **show mpls ip iprm counters**
- **show mpls ip iprm ldm**

# Feature Information for MPLS High Availability: Overview

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for MPLS High Availability: Overview

Feature Name	Releases	Feature Information
MPLS High Availability: Overview	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature provides an overview of the Multiprotocol Label Switching (MPLS) high availability (HA) features.  In 12.2(25)S, this feature was introduced on the Cisco 7500 series router.  In 12.2(28)SB, support was added for the Cisco 10000.  In 12.2(33)SRA, support was added for the Cisco 7600 series routers.  In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.





# MPLS High Availability: Command Changes

---

**First Published: August 11, 2004**

**Last Updated: August 21, 2007**

This feature module details changes to commands that are required to support updates to the Multiprotocol Label Switching (MPLS) High Availability (HA) feature.

In Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH, the MPLS control plane software is enhanced to work in MPLS HA environments. The changes made the control plane software more modular, which helps MPLS support MPLS HA applications. Some of the control plane software changes also made MPLS more scalable and flexible.

Changes to the MPLS Forwarding Infrastructure (MFI) and the Cisco Express Forwarding component introduced new commands and changed other existing commands. MFI replaced the Label Forwarding Information Base (LFIB) and is responsible for managing MPLS data structures used for forwarding.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for MPLS High Availability: Command Changes”](#) section on page 9.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Information About MPLS High Availability: Command Changes, page 2](#)
- [How to Configure MPLS High Availability: Command Changes, page 6](#)
- [Configuration Examples for MPLS High Availability: Command Changes, page 7](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Feature Information for MPLS High Availability: Command Changes, page 9](#)

## Information About MPLS High Availability: Command Changes

Before using MPLS High Availability features, you should understand the following concepts:

- [MPLS Replacement Commands for Tag-Switching Commands, page 2](#)
- [New Command Defaults, page 2](#)
- [MPLS MTU Command Changes, page 2](#)
- [Deleted Commands, page 3](#)
- [Replaced Commands, page 3](#)

## MPLS Replacement Commands for Tag-Switching Commands

Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, all tag-switching commands are obsoleted and are replaced with MPLS command versions. When you enter an obsolete tag-switching command, such as **tag-switching ip**, you receive the following message:

```
% Command accepted but obsolete, unreleased, or unsupported; see documentation
```

Use the MPLS version of the command instead, such as **mpls ip**.

Support for the tag-switching versions of commands will cease in a future release.

Configuration files that use the tag-switching version of the commands continue to operate. However, running configurations will display the new MPLS versions of the commands.

## New Command Defaults

Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA and 12.2(33)SXH, Label Distribution Protocol (LDP) is the default protocol. In other releases and trains, the default label distribution protocol is Tag Distribution Protocol (TDP). See the **mpls label protocol** (global configuration) command in the [NSF/SSO—MPLS LDP and MPLS LDP Graceful Restart](#) feature for more information.

## MPLS MTU Command Changes

The **mpls mtu** command has changed over the course of the several releases, starting in Cisco IOS Release 12.2(25)S. This section documents the changes implemented in Cisco IOS Release 12.2(25)S. For information about the changes implemented in Cisco IOS Releases 12.2(27)SBC and later releases, see the [MPLS MTU Command Changes](#) feature.

In Cisco IOS Release 12.2(25)S, if the interface MTU is less than 1524 bytes, you can set the maximum MPLS MTU to 24 bytes more than the interface MTU. For example, if the interface MTU is set to 1510 bytes, then you can set the maximum MPLS MTU to 1534 bytes (1510 + 24).

**Note**

Although you can set the MPLS MTU to a value greater than the interface MTU, it is recommended that you keep the MPLS MTU less than or equal to the interface MTU to prevent the hardware from dropping packets. A best practice is to set the interface MTU of the core-facing interface to a value greater than either the IP MTU or interface MTU of the edge-facing interface.

If the interface MTU is greater than or equal to 1524 bytes, then you can set the maximum MPLS MTU as high as the interface MTU. For example, if the interface MTU is set to 1600 bytes, then you can set the MPLS MTU to a maximum of 1600 bytes. If you set the MPLS MTU higher than the interface MTU, traffic is dropped.

For interfaces that do not allow you to configure the interface MTU value and the interface MTU is 1500 bytes, the MPLS MTU range is 64 to 1524 bytes.

If you upgrade to Cisco IOS Release 12.2(25)S from an earlier release and you have an MPLS MTU setting that does not conform to these guidelines, the MPLS MTU setting is not accepted by the system. If this happens, reconfigure the MPLS MTU setting to conform to the guidelines.

## Deleted Commands

The following commands are no longer available in Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH:

- **debug mpls adjacency**
- **debug mpls lfib cef**
- **debug mpls lfib enc**
- **debug mpls lfib lsp**
- **debug mpls lfib state**
- **debug mpls lfib struct**
- **debug mpls lfib fast-reroute**

## Replaced Commands

[Table 1](#) lists the commands that use the term tag-switching. Starting with Cisco IOS Releases 12.2(25)S, 12.2(28)SB, 12.2(33)SRA, and 12.2(33)SXH, these commands have been updated with MPLS terminology. Although the tag-switching versions of the commands are obsoleted, the tag-switching commands continue to work, but are not documented.

Please use the MPLS versions of the commands. If you issue a tag-switching command, you receive the following error:

```
% Command accepted but obsolete, unreleased, or unsupported; see documentation
```

For information about any of the MPLS commands in [Table 1](#) and [Table 2](#), see the *Cisco IOS Multiprotocol Label Switching Command Reference*.

[Table 1](#) alphabetically lists the MPLS commands used by the Cisco 7500 series routers that replaced the tag-switching commands.

**Table 1** *Cisco 7500 Series—MPLS Commands That Replaced Tag-Switching Commands*

<b>This MPLS Command Replaces</b>	<b>This Tag-Switching Command</b>
debug mpls atm-cos	debug tag-switching atm-cos
debug mpls atm-ldp api	debug tag-switching atm-tdp api
debug mpls atm-ldp routes	debug tag-switching atm-tdp routes
debug mpls atm-ldp states	debug tag-switching atm-tdp states
debug mpls events	debug tag-switching events
debug mpls ldp advertisements	debug tag-switching tdp advertisements
debug mpls ldp bindings	debug tag-switching tdp bindings
debug mpls ldp messages	debug tag-switching tdp pies
debug mpls ldp peer state-machine	debug tag-switching tdp peer state-machine
debug mpls ldp session io	debug tag-switching tdp session io
debug mpls ldp session state-machine	debug tag-switching tdp session state-machine
debug mpls ldp targeted-neighbors	debug tag-switching tdp directed-neighbors
debug mpls ldp transport connections	debug tag-switching tdp transport connections
debug mpls ldp transport events	debug tag-switching tdp transport events
debug mpls traffic-eng tunnels events	debug tag-switching tsp-tunnels events
debug mpls traffic-eng tunnels labels	debug tag-switching tsp-tunnels tagging
debug mpls traffic-eng tunnels signalling	debug tag-switching tsp-tunnels signalling
debug mpls xtagatm cross-connect	debug tag-switching xtagatm cross-connect
debug mpls xtagatm errors	debug tag-switching xtagatm errors
debug mpls xtagatm events	debug tag-switching xtagatm events
debug mpls xtagatm vc	debug tag-switching xtagatm vc
mpls atm control-vc	tag-switching atm control-vc
mpls atm cos	tag-switching atm cos
mpls atm disable-headend-vc	tag-switching atm disable-headend-vc
mpls atm multi-vc	tag-switching atm multi-vc
mpls atm vpi	tag-switching atm vpi
mpls atm vp-tunnel	tag-switching atm vp-tunnel
mpls cos-map	tag-switching cos-map
mpls ip (global configuration)	tag-switching ip (global configuration)
mpls ip (interface configuration)	tag-switching ip (interface configuration)
mpls ip default-route	tag-switching ip default-route
mpls ip propagate-ttl	tag-switching ip propagate-ttl
mpls label range	tag-switching tag-range downstream
mpls ldp advertise-labels	tag-switching advertise-tags
mpls ldp atm control-mode	tag-switching atm allocation-mode

**Table 1** *Cisco 7500 Series—MPLS Commands That Replaced Tag-Switching Commands (continued)*

This MPLS Command Replaces	This Tag-Switching Command
mpls ldp atm vc-merge	tag-switching atm vc-merge
mpls ldp discovery	tag-switching tdp discovery
mpls ldp holdtime	tag-switching tdp holdtime
mpls ldp maxhops	tag-switching atm maxhops
mpls mtu	tag-switching mtu
mpls prefix-map	tag-switching prefix-map
mpls request-labels for	tag-switching request-tags for
mpls traffic-eng tunnels	tag-switching tsp-tunnels
show mpls atm-ldp bindings	show tag-switching atm-tdp bindings
show mpls atm-ldp bindwait	show tag-switching atm-tdp bindwait
show mpls atm-ldp capability	show tag-switching atm-tdp capability
show mpls atm-ldp summary	show tag-switching atm-tdp summary
show mpls cos-map	show tag-switching cos-map
show mpls forwarding-table	show tag-switching forwarding-table show tag-switching forwarding vrf
show mpls interfaces	show tag-switching interfaces
show mpls ldp bindings	show tag-switching tdp bindings
show mpls ldp discovery	show tag-switching tdp discovery
show mpls ldp neighbors	show tag-switching tdp neighbors
show mpls ldp parameters	show tag-switching tdp parameters
show mpls prefix-map	show tag-switching prefix-map
show mpls traffic-eng tunnels	show tag-switching tsp-tunnels
tunnel mode mpls traffic-eng	tunnel mode tag-switching

Table 2 alphabetically lists the MPLS commands used by the Cisco 10000 series routers that replaced the tag-switching commands.

**Table 2** *Cisco 10000 Series—MPLS Commands That Replaced Tag-Switching Commands*

This MPLS Command Replaces	This Tag-Switching Command
debug mpls events	debug tag-switching events
debug mpls ldp advertisements	debug tag-switching tdp advertisements
debug mpls ldp bindings	debug tag-switching tdp bindings
debug mpls ldp messages	debug tag-switching tdp pies
debug mpls ldp peer state-machine	debug tag-switching tdp peer state-machine
debug mpls ldp session io	debug tag-switching tdp session io
debug mpls ldp session state-machine	debug tag-switching tdp session state-machine
debug mpls ldp targeted-neighbors	debug tag-switching tdp directed-neighbors



**Table 2** *Cisco 10000 Series—MPLS Commands That Replaced Tag-Switching Commands (continued)*

<b>This MPLS Command Replaces</b>	<b>This Tag-Switching Command</b>
debug mpls ldp transport connections	debug tag-switching tdp transport connections
debug mpls ldp transport events	debug tag-switching tdp transport events
debug mpls traffic-eng tunnels events	debug tag-switching tsp-tunnels events
debug mpls traffic-eng tunnels labels	debug tag-switching tsp-tunnels tagging
debug mpls traffic-eng tunnels signalling	debug tag-switching tsp-tunnels signalling
mpls ip (global configuration)	tag-switching ip (global configuration)
mpls ip (interface configuration)	tag-switching ip (interface configuration)
mpls ip default-route	tag-switching ip default-route
mpls ip propagate-ttl	tag-switching ip propagate-ttl
mpls label range	tag-switching tag-range downstream
mpls ldp advertise-labels	tag-switching advertise-tags
mpls ldp discovery	tag-switching tdp discovery
mpls ldp holdtime	tag-switching tdp holdtime
mpls ldp maxhops	tag-switching atm maxhops
mpls mtu	tag-switching mtu
mpls prefix-map	tag-switching prefix-map
mpls request-labels for	tag-switching request-tags for
mpls traffic-eng tunnels	tag-switching tsp-tunnels
show mpls forwarding-table	show tag-switching forwarding-table show tag-switching forwarding vrf
show mpls interfaces	show tag-switching interfaces
show mpls ldp bindings	show tag-switching tdp bindings
show mpls ldp discovery	show tag-switching tdp discovery
show mpls ldp neighbors	show tag-switching tdp neighbors
show mpls ldp parameters	show tag-switching tdp parameters
show mpls prefix-map	show tag-switching prefix-map
show mpls traffic-eng tunnels	show tag-switching tsp-tunnels
tunnel mode mpls traffic-eng	tunnel mode tag-switching

## How to Configure MPLS High Availability: Command Changes

There are no configuration tasks for this feature.

# Configuration Examples for MPLS High Availability: Command Changes

There are no configuration examples for this feature.

## Additional References

The following sections provide references related to the MPLS High Availability feature.

## Related Documents

Related Topic	Document Title
MPLS HA for VPNS	<a href="#">NSF/SSO-MPLS VPN</a>
MPLS HA for LDP	<a href="#">NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart</a>
MPLS HA and other applications	<a href="#">MPLS High Availability: Overview</a>
Stateful switchover	<a href="#">Stateful Switchover</a>
MPLS Label Distribution Protocol	<a href="#">MPLS Label Distribution Protocol (LDP)</a>
Cisco nonstop forwarding	<a href="#">Cisco Nonstop Forwarding</a>
MPLS MTU command changes implemented in Cisco IOS Releases 12.2(27)SBC and later releases.	<a href="#">MPLS MTU Command Changes</a>
Cisco IOS Release 12.4 commands	<a href="#">Cisco IOS Multiprotocol Label Switching Command Reference</a>

## Standards

Standard	Title
None	—

## MIBs

MIB	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

## RFCs

RFC	Title
None	—

## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls packets**
- **mpls mtu**
- **show atm vc**
- **show mpls forwarding-table**
- **show tech-support mpls**

# Feature Information for MPLS High Availability: Command Changes

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 3** Feature Information for MPLS High Availability: Command Changes

Feature Name	Releases	Feature Information
MPLS High Availability: Command Changes	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	This feature explains the MPLS commands that have been modified for the MPLS High Availability feature.  In 12.2(25)S, this feature was introduced on the Cisco 7500 series router.  In 12.2(28)SB, support was added for the Cisco 10000 series router.  In 12.2(33)SRA, support was added for the Cisco 7600 series router.  In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2007 Cisco Systems, Inc. All rights reserved.





## MPLS LDP Graceful Restart

---

When a router is configured with Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) Graceful Restart (GR), it assists a neighboring router that has MPLS LDP Stateful Switchover/Nonstop Forwarding (SSO/NSF) Support and Graceful Restart to recover gracefully from an interruption in service. In this Cisco IOS release, MPLS LDP GR functions strictly in helper mode, which means it can only help other routers that are enabled with MPLS SSO/NSF and GR to recover. If the router with LDP GR fails, its peer routers cannot help it recover.

### Notes:

- MPLS LDP SSO/NSF Support and Graceful Restart is supported in Cisco IOS Release 12.2(25)S. For brevity, this feature is called LDP SSO/NSF in this document.
- The MPLS LDP GR feature described in this document refers to helper mode.

When you enable MPLS LDP GR on a router that peers with an MPLS LDP SSO/NSF-enabled router, the SSO/NSF-enabled router can maintain its forwarding state when the LDP session between them is interrupted. While the SSO/NSF-enabled router recovers, the peer router forwards packets using stale information. This enables the SSO/NSF-enabled router to become operational more quickly.

### Feature History for MPLS LDP Graceful Restart

Release	Modification
12.0(29)S	The MPLS LDP Graceful Restart feature (in helper mode) was introduced.
12.3(14)T	This feature was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.

### Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Information About MPLS LDP Graceful Restart, page 2](#)
- [How to Configure MPLS LDP Graceful Restart, page 3](#)
- [Configuration Example for MPLS LDP Graceful Restart, page 6](#)
- [Additional References, page 10](#)
- [Command Reference, page 11](#)

## Information About MPLS LDP Graceful Restart

To configure MPLS LDP GR, you need to understand the following concepts:

- [How MPLS LDP Graceful Restart Works, page 2](#)
- [How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart, page 3](#)
- [What Happens If a Route Processor Does Not Have LDP Graceful Restart, page 3](#)

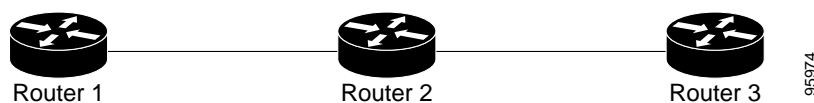
## How MPLS LDP Graceful Restart Works

MPLS LDP GR works in strict helper mode, which means it helps a neighboring route processor that has MPLS LDP SSO/NSF to recover from disruption in service without losing its MPLS forwarding state. The disruption in service could be the result of a TCP or UDP event or the stateful switchover of a route processor. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding states are recovered.

In the topology shown in [Figure 1](#), the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- Router 2 has been configured with MPLS LDP SSO/NSF. Routers 1 and 3 have been configured with MPLS LDP GR.
- A label switched path (LSP) has been established between Router 1 and Router 3.

**Figure 1**      *Example of a Network Using LDP Graceful Restart*



The following process shows how Routers 1 and 3, which have been configured with LDP GR help Router 2, which has been configured with LDP SSO/NSF recover from a disruption in service:

1. Router 1 notices an interruption in service with Router 2. (Router 3 also performs the same actions in this process.)
2. Router 1 marks all the label bindings from Router 2 as stale, but it continues to use the bindings for MPLS forwarding.

Router 1 reestablishes an LDP session with Router 2, but keeps its stale label bindings. If you issue a **show mpls ldp neighbor** command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.

- Both routers readvertise their label binding information. If Router 1 relearns a label from Router 2 after the session has been established, the stale flags are removed. The **show mpls forwarding-table** command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various graceful restart timers. See the following commands for more information:

- mpls ldp graceful-restart timers neighbor-liveness**
- mpls ldp graceful-restart timers max-recovery**

## How a Route Processor Advertises That It Supports MPLS LDP Graceful Restart

A route processor that is configured to perform MPLS LDP GR includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The route processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the route processor is configured to perform MPLS LDP GR.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. In this release, the timer is set to 0, which indicates that if the local router fails, its peers should not wait for it to recover. The timer setting indicates that the local router is working in helper mode.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

## What Happens If a Route Processor Does Not Have LDP Graceful Restart

If two route processors establish an LDP session and one route processor is not configured for MPLS LDP GR, the two route processors create a normal LDP session but do not have the ability to perform MPLS LDP GR. Both route processors must be configured for MPLS LDP GR.

## How to Configure MPLS LDP Graceful Restart

This section contains the following procedures:

- [Configuring MPLS LDP Graceful Restart, page 3](#) (required)
- [Verifying the Configuration, page 5](#) (optional)

## Configuring MPLS LDP Graceful Restart

You must enable MPLS LDP GR on all route processors for an LDP session to be preserved during an interruption in service.



MPLS LDP GR is enabled globally. When you enable MPLS LDP GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform MPLS LDP GR.

## Restrictions

- MPLS LDP GR is supported in strict helper mode.
- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- MPLS LDP SSO/NSF is supported in IOS Release 12.2(25)S. It is not supported in this release.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp graceful-restart**
5. **interface type slot/port**
6. **mpls ip**
7. **mpls label protocol {ldp | tdp | both}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables Cisco Express Forwarding (CEF).
Step 4	<b>mpls ldp graceful-restart</b>  <b>Example:</b> Router(config)# mpls ldp graceful-restart	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	<b>interface type slot/port</b>  <b>Example:</b> Router(config)# interface pos 3/0	Specifies an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 6	<code>mpls ip</code>  <b>Example:</b> Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	<code>mpls label protocol {ldp   tdp   both}</code>  <b>Example:</b> Router(config-if)# mpls label protocol ldp	Configures the use of LDP for an interface. You must use LDP.

**Note**

You can also issue the **mpls label protocol ldp** command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

## Verifying the Configuration

The following commands help verify that MPLS LDP GR has been configured correctly:

<b>show mpls ldp neighbor with the graceful-restart keyword</b>	Displays the Graceful Restart information for LDP sessions.
<code>show mpls ldp graceful-restart</code>	Displays Graceful Restart sessions and session parameters.

# Configuration Example for MPLS LDP Graceful Restart

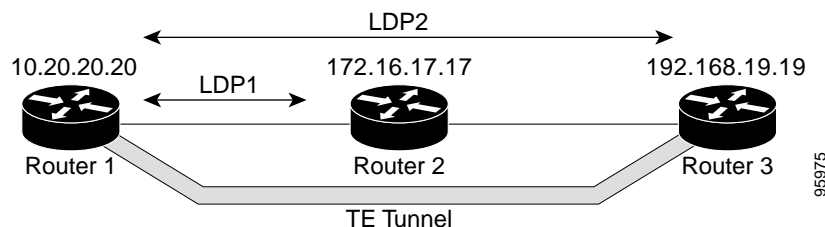
Figure 2 shows a configuration where MPLS LDP GR is enabled on Router 1 and MPLS LDP SSO/NSF is enabled on Routers 2 and 3. In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a traffic engineering tunnel using Router 2.



**Note**

MPLS LDP SSO/NSF is supported in Cisco IOS Release 12.2(25)S. It is not supported in this release.

**Figure 2** *MPLS LDP Graceful Restart Configuration Example*



## Router 1 configured with LDP GR:

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
  ip address 20.20.20.20 255.255.255.255
  no ip directed-broadcast
  no ip mroute-cache
!
interface Tunnell
  ip unnumbered Loopback0
  no ip directed-broadcast
  mpls label protocol ldp
  mpls ip
  tunnel destination 19.19.19.19
  tunnel mode mpls traffic-eng
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng priority 7 7
  tunnel mpls traffic-eng bandwidth 500
  tunnel mpls traffic-eng path-option 1 dynamic
!
interface ATM5/1/0
  no ip address
  no ip directed-broadcast
  atm clock INTERNAL
  
```

```

        no atm enable-ilmi-trap
        no atm ilmi-keepalive
    !
interface ATM5/1/0.5 point-to-point
    ip address 12.0.0.2 255.0.0.0
    no ip directed-broadcast
    no atm enable-ilmi-trap
    pvc 6/100
        encapsulation aal5snap
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip
    ip rsvp bandwidth 1000
!
router ospf 100
    log-adjacency-changes
    redistribute connected
    network 12.0.0.0 0.255.255.255 area 100
    network 20.20.20.20 0.0.0.0 area 100
    mpls traffic-eng router-id Loopback0
    mpls traffic-eng area 100

```

### Router 2 configured with LDP SSO/NSF:

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
redundancy
    mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
    ip address 17.17.17.17 255.255.255.255
    no ip directed-broadcast
!
interface ATM4/0/0
    no ip address
    no ip directed-broadcast
    no ip mroute-cache
    atm clock INTERNAL
    atm sonet stm-1
    no atm enable-ilmi-trap
    no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
    ip address 12.0.0.1 255.0.0.0
    no ip directed-broadcast
    no atm enable-ilmi-trap
    pvc 6/100
        encapsulation aal5snap
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip

```

```

        ip rsvp bandwidth 1000
    !
interface POS5/1/0
    ip address 11.0.0.1 255.0.0.0
    no ip directed-broadcast
    encapsulation ppp
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip
    no peer neighbor-route
    clock source internal
    ip rsvp bandwidth 1000
!
router ospf 100
    log-adjacency-changes
    redistribute connected
    nsf enforce global
    network 11.0.0.0 0.255.255.255 area 100
    network 12.0.0.0 0.255.255.255 area 100
    network 17.17.17.17 0.0.0.0 area 100
    mpls traffic-eng router-id Loopback0
    mpls traffic-eng area 100
!
ip classless

```

#### Router 3 configured with LDP SSO/NSF:

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
!
redundancy
    mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 11.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
    ip address 19.19.19.19 255.255.255.255
    no ip directed-broadcast
!
interface POS1/0
    ip address 11.0.0.2 255.0.0.0
    no ip directed-broadcast
    encapsulation ppp
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip
    no peer neighbor-route
    clock source internal
    ip rsvp bandwidth 1000

```

```
!  
router ospf 100  
    log-adjacency-changes  
    redistribute connected  
    nsf enforce global  
    network 11.0.0.0 0.255.255.255 area 100  
    network 19.19.19.19 0.0.0.0 area 100  
    mpls traffic-eng router-id Loopback0  
    mpls traffic-eng area 100  
!  
ip classless
```

# Additional References

The following sections provide references related to MPLS LDP GR.

## Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol	<a href="#">MPLS Label Distribution Protocol (LDP)</a>

## Standards

Standards	Title
None	—

## MIBs

MIBs <sup>1</sup>	MIBs Link
<ul style="list-style-type: none"> <li>MPLS Label Distribution Protocol MIB Version 8 Upgrade</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

1. Not all supported MIBs are listed.

## RFCs

RFCs <sup>1</sup>	Title
RFC 3036	<i>LDP Specification</i>
RFC 3478	<i>Graceful Restart Mechanism for Label Distribution</i>

1. Not all supported RFCs are listed.

## Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp graceful-restart**
- **mpls ldp graceful-restart**
- **mpls ldp graceful-restart timers max-recovery**
- **mpls ldp graceful-restart timers neighbor-liveness**
- **show mpls ip binding**
- **show mpls ldp bindings**
- **show mpls ldp graceful-restart**
- **show mpls ldp neighbor**

---

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

---

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

---

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

© 2007 Cisco Systems, Inc. All rights reserved.







# NSF/SSO - MPLS LDP and LDP Graceful Restart

---

**First Published: August 16, 2004**

**Last Updated: August 21, 2007**

Cisco Nonstop Forwarding with Stateful Switchover provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) uses SSO, NSF, and graceful restart to allow a Route Processor to recover from disruption in control plane service (specifically, the LDP component) without losing its MPLS forwarding state. LDP NSF works with LDP sessions between directly connected peers and with peers that are not directly connected (targeted sessions).



## Note

---

In this document, the NSF/SSO - MPLS LDP and LDP Graceful Restart feature is called LDP NSF for brevity.

---

## Finding Feature Information in This Module

*Your Cisco IOS software release may not support all of the features documented in this module.* To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for NSF/SSO - MPLS LDP and LDP Graceful Restart](#)” section on [page 16](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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



---

**Americas Headquarters:**

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

© 2007 Cisco Systems, Inc. All rights reserved.

# Contents

- [Prerequisites for NSF/SSO - MPLS LDP and LDP Graceful Restart, page 2](#)
- [Restrictions for NSF/SSO - MPLS LDP and LDP Graceful Restart, page 2](#)
- [Information About NSF/SSO - MPLS LDP and LDP Graceful Restart, page 2](#)
- [How to Configure and Use NSF/SSO - MPLS LDP and LDP Graceful Restart, page 5](#)
- [Configuration Examples for LDP NSF, page 8](#)
- [Additional References, page 14](#)
- [Command Reference, page 15](#)
- [Feature Information for NSF/SSO - MPLS LDP and LDP Graceful Restart, page 16](#)

## Prerequisites for NSF/SSO - MPLS LDP and LDP Graceful Restart

For information about supported hardware, see the release notes for your platform.

MPLS high availability (HA) requires that neighbor networking devices be NSF-aware.

To perform LDP NSF, Route Processors must be configured for SSO. See the [Stateful Switchover](#) feature module for more information:

You must enable nonstop forwarding on the routing protocols running between the provider (P) routers, provider edge (PE) routers, and customer edge (CE) routers. The routing protocols are:

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

See the [Cisco Nonstop Forwarding](#) feature module for more information.

## Restrictions for NSF/SSO - MPLS LDP and LDP Graceful Restart

LDP NSF has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- LDP NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.

## Information About NSF/SSO - MPLS LDP and LDP Graceful Restart

To configure LDP NSF, you need to understand the following concepts:

- [How NSF/SSO - MPLS LDP and LDP Graceful Restart Works, page 3](#)
- [How a Route Processor Advertises That It Supports NSF/SSO - MPLS LDP and LDP Graceful Restart, page 4](#)
- [Checkpointing, page 5](#)

## How NSF/SSO - MPLS LDP and LDP Graceful Restart Works

LDP NSF allows a Route Processor to recover from disruption in service without losing its MPLS forwarding state. LDP NSF works under the following circumstances:

- **LDP restart**—An LDP Restart occurs after an SSO event interrupts LDP communication with all LDP neighbors. If the Route Processors are configured with LDP NSF, the backup Route Processor retains the MPLS forwarding state and reestablishes communication with the LDP neighbors. Then the Route Processor ensures that the MPLS forwarding state is recovered.
- **LDP session reset**—An LDP session reset occurs after an individual LDP session has been interrupted, but the interruption is not due to an SSO event. The LDP session might have been interrupted due to a TCP or UDP communication problem. If the Route Processor is configured with MPLS LDP NSF support and graceful restart, the Route Processor associates a new session with the previously interrupted session. The LDP bindings and MPLS forwarding states are recovered when the new session is established.

If an SSO event occurs on an LSR, that LSR performs an LDP restart. The adjacent LSRs perform an LDP session reset.

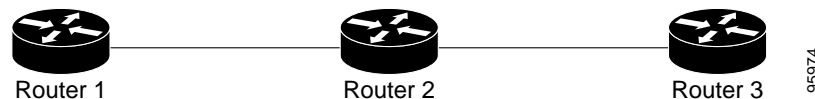
See the following section for more information about LDP restart and reset.

### What Happens During an LDP Restart and an LDP Session Reset

In the topology shown in [Figure 1](#), the following elements have been configured:

- LDP sessions are established between Router 1 and Router 2, as well as between Router 2 and Router 3.
- A label switched path (LSP) has been established between Router 1 and Router 3.
- The routers have been configured with LDP NSF.

**Figure 1** Example of a Network Using LDP Graceful Restart



The following process shows how LDP recovers when one of the routers fails:

1. When a Route Processor fails on Router 2, communications between the routers is interrupted.
2. Router 1 and Router 3 mark all the label bindings from Router 2 as stale, but they continue to use the bindings for MPLS forwarding.
3. Router 1 and Router 3 attempt to reestablish an LDP session with Router 2.
4. Router 2 restarts and marks all of its forwarding entries as stale. If you issue a **show mpls ldp graceful-restart** command, the command output includes the following line:  

```
LDP is restarting gracefully.
```
5. Router 1 and Router 3 reestablish LDP sessions with Router 2, but they keep their stale label bindings. If you issue a **show mpls ldp neighbor** command with the **graceful-restart** keyword, the command output displays the recovering LDP sessions.

6. All three routers readvertise their label binding information. If a label has been relearned after the session has been established, the stale flags are removed. The **show mpls forwarding-table** command displays the information in the MPLS forwarding table, including the local label, outgoing label or VC, prefix, label-switched bytes, outgoing interface, and next hop.

You can set various timers to limit how long the routers wait for an LDP session to be reestablished before restarting the router. See the following commands for more information:

- [mpls ldp graceful-restart timers forwarding-holding](#)
- [mpls ldp graceful-restart timers max-recovery](#)
- [mpls ldp graceful-restart timers neighbor-liveness](#)

## How a Route Processor Advertises That It Supports NSF/SSO - MPLS LDP and LDP Graceful Restart

A Route Processor that is configured to perform LDP NSF includes the Fault Tolerant (FT) Type Length Value (TLV) in the LDP initialization message. The Route Processor sends the LDP initialization message to a neighbor to establish an LDP session.

The FT session TLV includes the following information:

- The Learn from Network (L) flag is set to 1, which indicates that the Route Processor is configured to perform LDP Graceful Restart.
- The Reconnect Timeout field shows the time (in milliseconds) that the neighbor should wait for a reconnection if the LDP session is lost. This field is set to 120 seconds and cannot be configured.
- The Recovery Time field shows the time (in milliseconds) that the neighbor should retain the MPLS forwarding state during a recovery. If a neighbor did not preserve the MPLS forwarding state before the restart of the control plane, the neighbor sets the recovery time to 0.

## What Happens if a Route Processor Does Not Have LDP Graceful Restart

If a Route Processor is not configured for MPLS LDP Graceful Restart and it attempts to establish an LDP session with a Route Processor that is configured with LDP Graceful Restart, the following events occur:

1. The Route Processor that is configured with MPLS LDP Graceful Restart sends an initialization message that includes the FT session TLV value to the Route Processor that is not configured with MPLS LDP Graceful Restart.
2. The Route Processor that is not configured for MPLS LDP Graceful Restart receives the LDP initialization message and discards the FT session TLV.
3. The two Route Processors create a normal LDP session but do not have the ability to perform MPLS LDP Graceful Restart.

You must enable all Route Processors with MPLS LDP Graceful Restart for an LDP session to be preserved during an interruption in service.

## Checkpointing

Checkpointing is a function that copies state information from the active Route Processor to the backup Route Processor, thereby ensuring that the backup Route Processor has the latest information. If the active Route Processor fails, the backup Route Processor can take over.

For the LDP NSF feature, the checkpointing function copies the active Route Processor's LDP local label bindings to the backup Route Processor. The active Route Processor sends updates to the backup Route Processor when local label bindings are modified as a result of routing changes.

**Note**

Local label bindings that are allocated by BGP and null local label bindings are not included in the checkpointing operation.

The checkpointing function is enabled by default.

To display checkpointing data, issue the **show mpls ldp graceful-restart** command on the active Route Processor.

To check that the active and backup Route Processors have identical copies of the local label bindings, you can issue the **show mpls ldp bindings** command with the **detail** keyword on the active and backup Route Processors. This command displays the local label bindings that have been saved. The active Route Processor and the backup Route Processor should have the same local label bindings.

## Troubleshooting Tips

You can use the **debug mpls ldp graceful-restart** command to enable the display of MPLS LDP checkpoint events and errors.

## How to Configure and Use NSF/SSO - MPLS LDP and LDP Graceful Restart

- [Configuring MPLS LDP Graceful Restart, page 5](#) (required)
- [Verifying the Configuration, page 7](#) (optional)

## Configuring MPLS LDP Graceful Restart

MPLS LDP Graceful Restart (GR) is enabled globally. When you enable LDP GR, it has no effect on existing LDP sessions. LDP GR is enabled for new sessions that are established after the feature has been globally enabled.

## Prerequisites

- Route Processors must be configured for SSO. See the [Stateful Switchover](#) feature module for more information:
- You must enable Nonstop Forwarding on the routing protocols running between the P, PE, routers, and CE routers. See the [Cisco Nonstop Forwarding](#) feature module for more information.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp graceful-restart**
5. **interface type slot/port**
6. **mpls ip**
7. **mpls label protocol {ldp | tdp | both}**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables distributed Cisco Express Forwarding on Cisco 7500 series routers. Distributes Cisco Express Forwarding information to line cards.  <b>Note</b> For the Cisco 10000 series routers, IP Cisco Express Forwarding is on by default and it cannot be disabled.
Step 4	<b>mpls ldp graceful-restart</b>  <b>Example:</b> Router (config)# mpls ldp graceful-restart	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.
Step 5	<b>interface type slot/port</b>  <b>Example:</b> Router(config)# interface pos 3/0	Specifies an interface and enters interface configuration mode.
Step 6	<b>mpls ip</b>  <b>Example:</b> Router(config-if)# mpls ip	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	<b>mpls label protocol {ldp   tdp   both}</b>  <b>Example:</b> Router(config-if)# mpls label protocol ldp	Configures the use of LDP for an interface. You must use LDP. You can also issue the <b>mpls label protocol ldp</b> command in global configuration mode, which enables LDP on all interfaces configured for MPLS.

## Verifying the Configuration

Use the following procedure to verify that MPLS LDP Graceful Restart has been configured correctly.

### SUMMARY STEPS

1. **show mpls ldp graceful-restart**
2. **show mpls ldp neighbor graceful restart**
3. **show mpls ldp checkpoint**

### DETAILED STEPS

---

**Step 1 show mpls ldp graceful-restart**

The command output displays Graceful Restart sessions and session parameters:

```
Router# show mpls ldp graceful-restart

LDP Graceful Restart is enabled
Neighbor Liveness Timer: 5 seconds
Max Recovery Time: 200 seconds
Down Neighbor Database (0 records):
Graceful Restart-enabled Sessions:
VRF default:

    Peer LDP Ident: 10.18.18.18:0, State: estab
    Peer LDP Ident: 10.17.17.17:0, State: estab
```

**Step 2 show mpls ldp neighbor graceful restart**

The command output displays the Graceful Restart information for LDP sessions:

```
Router# show mpls ldp neighbor graceful-restart

Peer LDP Ident: 10.20.20.20:0; Local LDP Ident 10.17.17.17:0
  TCP connection: 10.20.20.20.16510 - 10.17.17.17.646
  State: Oper; Msgs sent/rcvd: 8/18; Downstream
  Up time: 00:04:39
  Graceful Restart enabled; Peer reconnect time (msecs): 120000
Peer LDP Ident: 10.19.19.19:0; Local LDP Ident 10.17.17.17:0
  TCP connection: 10.19.19.19.11007 - 10.17.17.17.646
  State: Oper; Msgs sent/rcvd: 8/38; Downstream
  Up time: 00:04:30
  Graceful Restart enabled; Peer reconnect time (msecs): 120000
```

**Step 3 show mpls ldp checkpoint**

The command output displays the summary of the checkpoint information:

```
Router# show mpls ldp checkpoint

Checkpoint status: dynamic-sync
Checkpoint resend timer: not running
5 local bindings in add-skipped
9 local bindings in added
1 of 15+ local bindings in none
```



# Configuration Examples for LDP NSF

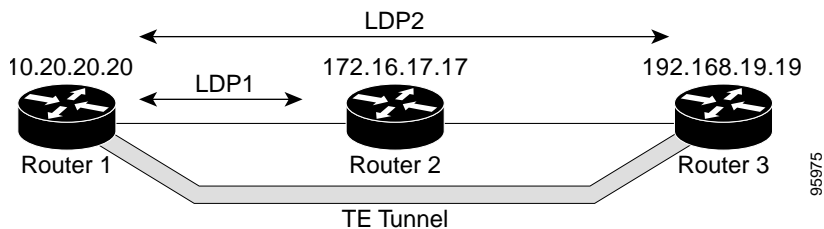
This section contains the following examples:

- [Configuring NSF/SSO - MPLS LDP and LDP Graceful Restart: Example, page 8](#)

## Configuring NSF/SSO - MPLS LDP and LDP Graceful Restart: Example

The following configuration example shows the LDP NSF feature configured on three routers. (See [Figure 2](#).) In this configuration example, Router 1 creates an LDP session with Router 2. Router 1 also creates a targeted session with Router 3 through a TE tunnel using Router 2.

**Figure 2** MPLS LDP: NSF/SSO Support and Graceful Restart Configuration Example



### Router 1—Cisco 7500 Series

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz

redundancy
mode sso
ip subnet-zero
ip cef
mpls label range 16 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.20.20.20 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
 mpls label protocol ldp
 mpls ip
 tunnel destination 10.19.19.19
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 500
 tunnel mpls traffic-eng path-option 1 dynamic

```

```

!
interface ATM5/1/0
    no ip address
    no ip directed-broadcast
    atm clock INTERNAL
    no atm enable-ilmi-trap
    no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
    ip address 172.17.0.2 255.255.0.0
    no ip directed-broadcast
    no atm enable-ilmi-trap
    pvc 6/100
        encapsulation aal5snap
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip
    ip rsvp bandwidth 1000
!
router ospf 100
    log-adjacency-changes
    redistribute connected
    nsf enforce global
    network 172.17.0.0 0.255.255.255 area 100
    network 172.20.20.20 0.0.0.0 area 100
    mpls traffic-eng router-id Loopback0
    mpls traffic-eng area 100

```

### Router 2—Cisco 7500 Series

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz

redundancy
mode sso
!
ip cef
no ip domain-lookup
mpls label range 17 10000 static 10001 1048575
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
no mpls advertise-labels
mpls ldp router-id Loopback0 force
!
interface Loopback0
    ip address 172.18.17.17 255.255.255.255
    no ip directed-broadcast
!
interface ATM4/0/0
    no ip address
    no ip directed-broadcast
    no ip mroute-cache
    atm clock INTERNAL
    atm sonet stm-1
    no atm enable-ilmi-trap
    no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
    ip address 172.17.0.1 255.255.0.0
    no ip directed-broadcast

```

```

        no atm enable-ilmi-trap
        pvc 6/100
            encapsulation aal5snap
        mpls label protocol ldp
        mpls traffic-eng tunnels
        mpls ip
        ip rsvp bandwidth 1000
    !
interface POS5/1/0
    ip address 10.0.0.1 255.0.0.0
    no ip directed-broadcast
    encapsulation ppp
    mpls label protocol ldp
    mpls traffic-eng tunnels
    mpls ip
    no peer neighbor-route
    clock source internal
    ip rsvp bandwidth 1000
!
router ospf 100
    log-adjacency-changes
    nsf enforce global
    redistribute connected
    network 10.0.0.0 0.255.255.255 area 100
    network 172.17.0.0 0.255.255.255 area 100
    network 172.18.17.17 0.0.0.0 area 100
    mpls traffic-eng router-id Loopback0
    mpls traffic-eng area 100
!
ip classless

```

### Router 3—Cisco 7500 Series

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz

redundancy
mode sso
!
ip subnet-zero
ip cef
!
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp neighbor 10.11.11.11 targeted ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
mpls traffic-eng tunnels
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp discovery directed-hello interval 12
mpls ldp discovery directed-hello holdtime 130
mpls ldp discovery directed-hello accept
mpls ldp router-id Loopback0 force
!
interface Loopback0
    ip address 172.19.19.19 255.255.255.255
    no ip directed-broadcast
!
interface POS1/0
    ip address 10.0.0.2 255.0.0.0
    no ip directed-broadcast
    encapsulation ppp

```

```

mpls label protocol ldp
mpls traffic-eng tunnels
mpls ip
no peer neighbor-route
clock source internal
ip rsvp bandwidth 1000
!
router ospf 100
  log-adjacency-changes
  nsf enforce global
  redistribute connected
  network 10.0.0.0 0.255.255.255 area 100
  network 172.19.19.19 0.0.0.0 area 100
  mpls traffic-eng router-id Loopback0
  mpls traffic-eng area 100
!
ip classless

```

### Router 1—Cisco 10000 Series

```

boot system flash:c10k2-p11-mz

redundancy
mode sso
ip subnet-zero
ip cef
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
  ip address 172.20.20.20 255.255.255.255
  no ip directed-broadcast
  no ip mroute-cache
!
interface ATM5/1/0
  no ip address
  no ip directed-broadcast
  atm clock INTERNAL
  no atm enable-ilmi-trap
  no atm ilmi-keepalive
!
interface ATM5/1/0.5 point-to-point
  ip address 172.18.0.2 255.255.0.0
  no ip directed-broadcast
  no atm enable-ilmi-trap
  pvc 6/100
    encapsulation aal5snap
  mpls label protocol ldp
  mpls ip
!
router ospf 100
  log-adjacency-changes
  redistribute connected
  nsf enforce global
  network 172.18.0.0 0.255.255.255 area 100
  network 172.20.20.20 0.0.0.0 area 100

```

### Router 2—Cisco 10000 Series

```

boot system flash:c10k2-p11-mz

```

```

redundancy
mode sso
!
ip cef
no ip domain-lookup
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
 ip address 172.17.17.17 255.255.255.255
 no ip directed-broadcast
!
interface ATM4/0/0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 atm clock INTERNAL
 atm sonet stm-1
 no atm enable-ilmi-trap
 no atm ilmi-keepalive
!
interface ATM4/0/0.5 point-to-point
 ip address 172.18.0.1 255.255.0.0
 no ip directed-broadcast
 no atm enable-ilmi-trap
 pvc 6/100
  encapsulation aal5snap
 mpls label protocol ldp
 mpls ip
!
interface POS5/1/0
 ip address 10.0.0.1 255.0.0.0
 no ip directed-broadcast
 encapsulation ppp
 mpls label protocol ldp
 mpls ip
 no peer neighbor-route
 clock source internal
!
router ospf 100
 log-adjacency-changes
 nsf enforce global
 redistribute connected
 network 10.0.0.0 0.255.255.255 area 100
 network 172.18.0.0 0.255.255.255 area 100
 network 172.17.17.17 0.0.0.0 area 100
 mpls traffic-eng router-id Loopback0
!
ip classless

```

### Router 3—Cisco 10000 Series

```
boot system flash:c10k2-pl1-mz
```

```

redundancy
mode sso
!
ip subnet-zero
ip cef
!

```

```
no ip finger
no ip domain-lookup
mpls label protocol ldp
mpls ldp logging neighbor-changes
mpls ldp graceful-restart
no mpls traffic-eng auto-bw timers frequency 0
mpls ldp router-id Loopback0 force
!
interface Loopback0
    ip address 172.19.19.19 255.255.255.255
    no ip directed-broadcast
!
interface POS1/0
    ip address 10.0.0.2 255.0.0.0
    no ip directed-broadcast
    encapsulation ppp
    mpls label protocol ldp
    mpls ip
    no peer neighbor-route
    clock source internal
!
router ospf 100
    log-adjacency-changes
    nsf enforce global
    redistribute connected
    network 10.0.0.0 0.255.255.255 area 100
    network 172.19.19.19 0.0.0.0 area 100
    mpls traffic-eng router-id Loopback0
!
ip classless
```

## Additional References

The following sections provide references related to the NSF/SSO - MPLS LDP and LDP Graceful Restart feature.

### Related Documents

Related Topic	Document Title
Stateful switchover	<a href="#"><i>Stateful Switchover</i></a>
MPLS Label Distribution Protocol	<a href="#"><i>MPLS Label Distribution Protocol (LDP)</i></a>
Cisco nonstop forwarding	<a href="#"><i>Cisco Nonstop Forwarding</i></a>

### Standards

Standard	Title
None	—

### MIBs

MIB	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
RFC 3036	LDP Specification
RFC 3478	Graceful Restart Mechanism for Label Distribution

## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug mpls ldp graceful-restart**
- **mpls label protocol (global configuration)**
- **mpls ldp graceful-restart**
- **mpls ldp graceful-restart timers forwarding-holding**
- **mpls ldp graceful-restart timers max-recovery**
- **mpls ldp graceful-restart timers neighbor-liveness**
- **show mpls ip binding**
- **show mpls ldp bindings**
- **show mpls ldp checkpoint**
- **show mpls ldp graceful-restart**
- **show mpls ldp neighbor**



# Feature Information for NSF/SSO - MPLS LDP and LDP Graceful Restart

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for NSF/SSO - MPLS LDP and LDP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO - MPLS LDP and LDP Graceful Restart	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	LDP NSF allows a Route Processor to recover from disruption in service without losing its MPLS forwarding state.  In 12.2(25)S, this feature was introduced on Cisco 7500 series routers.  In 12.2(28)SB, this feature was integrated into Cisco IOS Release 12.2(28)SB and implemented on Cisco 10000 series routers.  In 12.2(33)SRA, this feature was integrated into Cisco IOS Release 12.2(33)SRA.  In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.





# NSF/SSO—MPLS VPN

---

**First Published: August 11, 2004**

**Last Updated: August 21, 2007**

The NSF/SSO—MPLS VPN feature allows a provider edge (PE) router or Autonomous System Border Router (ASBR) (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor (RP) restarts. This feature module describes how to enable Nonstop Forwarding in MPLS VPN networks, including the following types of VPNs:

- Basic MPLS VPNs
- MPLS VPN—Carrier Supporting Carrier
- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Interautonomous Systems
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for NSF/SSO—MPLS VPN”](#) section on page 51.

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for NSF/SSO—MPLS VPN, page 2](#)
- [Restrictions for NSF/SSO—MPLS VPN, page 2](#)
- [Information About NSF/SSO—MPLS VPN, page 2](#)
- [How to Configure NSF/SSO—MPLS VPN, page 4](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for NSF/SSO—MPLS VPN](#), page 8
- [Additional References](#), page 49
- [Command Reference](#), page 50
- [Feature Information for NSF/SSO—MPLS VPN](#), page 51

## Prerequisites for NSF/SSO—MPLS VPN

The NSF/SSO—MPLS VPN feature has the following prerequisites:

For information about supported hardware, see the release notes for your platform.

Before enabling Stateful Switchover (SSO), you must enable MPLS Label Distribution Protocol (LDP) Graceful Restart if you use LDP in the core or in the MPLS VPN routing and forwarding instance in an MPLS VPN Carrier Supporting Carrier configuration. See the [NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart](#) feature module for more information.

You must enable NSF on the routing protocols running between the provider (P) routers, PE routers, and customer edge (CE) routers. The routing protocols are:

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

Cisco nonstop forwarding support must be configured on the routers for Cisco Express Forwarding. See the [Cisco Nonstop Forwarding](#) feature module for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. Configuration information is included in the [Configuring MPLS VPNs](#) feature module.

## Restrictions for NSF/SSO—MPLS VPN

The NSF/SSO—MPLS VPN feature has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- The NSF/SSO—MPLS VPN feature requires that neighbor networking devices be NSF-aware. Peer routers must support the graceful restart of the protocol used to communicate with the NSF/SSO—MPLS VPN-capable router.
- The NSF/SSO—MPLS VPN feature cannot be configured on label-controlled ATM (LC-ATM) interfaces.

## Information About NSF/SSO—MPLS VPN

To configure NSF/SSO—MPLS VPN, you need to understand the following concepts:

- [Elements That Enable NSF/SSO—MPLS VPN to Work](#), page 3
- [How VPN Prefix Information Is Checkpointed to the Backup Route Processor](#), page 3
- [How BGP Graceful Restart Preserves Prefix Information During a Restart](#), page 3
- [What Happens If a Router Does Not Have NSF/SSO—MPLS VPN Enabled](#), page 4

## Elements That Enable NSF/SSO—MPLS VPN to Work

VPN NSF requires several elements to work:

- VPN NSF uses the BGP Graceful Restart mechanisms defined in the Graceful Restart Internet Engineering Task Force (IETF) specifications and in the *Cisco Nonstop Forwarding* feature module. BGP Graceful Restart allows a router to create MPLS forwarding entries for VPNv4 prefixes in NSF mode. The forwarding entries are preserved during a restart. BGP also saves prefix and corresponding label information and recovers the information after a restart.
- The NSF/SSO—MPLS VPN feature also uses NSF for the label distribution protocol in the core network (either MPLS Label Distribution Protocol, traffic engineering, or static labeling).
- The NSF/SSO—MPLS VPN feature uses NSF for the Interior Gateway Protocol (IGP) used in the core (OSPF or IS-IS).
- The NSF/SSO—MPLS VPN feature uses NSF for the routing protocols between the PE and customer CE routers.

## How VPN Prefix Information Is Checkpointed to the Backup Route Processor

When BGP allocates local labels for prefixes, it checkpoints the local label binding in the backup Route Processor. The checkpointing function copies state information from the active Route Processor to the backup Route Processor, thereby ensuring that the backup Route Processor has an identical copy of the latest information. If the active Route Processor fails, the backup Route Processor can take over with no interruption in service. Checkpointing begins when the active Route Processor does a bulk synchronization, which copies all of the local label bindings to the backup Route Processor. After that, the active Route Processor dynamically checkpoints individual prefix label bindings when a label is allocated or freed. This allows forwarding of labeled packets to continue before BGP reconverges.

## How BGP Graceful Restart Preserves Prefix Information During a Restart

When a router that is capable of BGP Graceful Restart loses connectivity, the following happens to the restarting router:

1. The router establishes BGP sessions with other routers and relearns the BGP routes from other routers that are also capable of Graceful Restart. The restarting router waits to receive updates from the neighboring routers. When the neighboring routers send end-of-Routing Information Base (RIB) markers to indicate that they are done sending updates, the restarting router starts sending its own updates.
2. The restarting router accesses the checkpoint database to find the label that was assigned for each prefix. If it finds the label, it advertises it to the neighboring router. If it does not find the label, it allocates a new label and advertises it.
3. The restarting router removes any stale prefixes after a timer for stale entries expires.

When a peer router that is capable of BGP Graceful Restart encounters a restarting router, it does the following:

1. The peer router sends all of the routing updates to the restarting router. When it has finished sending updates, the peer router sends an end-of RIB marker to the restarting router.
2. The peer router does not immediately remove the BGP routes learned from the restarting router from its BGP routing table. As it learns the prefixes from the restarting router, the peer refreshes the stale routes if the new prefix and label information matches the old information.

## What Happens If a Router Does Not Have NSF/SSO—MPLS VPN Enabled

If a router is not configured for the NSF/SSO—MPLS VPN feature and it attempts to establish a BGP session with a router that is configured with the NSF/SSO—MPLS VPN feature, the two routers create a normal BGP session but do not have the ability to perform the NSF/SSO—MPLS VPN feature.

## How to Configure NSF/SSO—MPLS VPN

This section contains the following procedures:

- [Configuring NSF Support for Basic VPNs, page 4](#) (required)
- [Configuring NSF Support for MPLS VPN Interfaces That Use BGP as the Label Distribution Protocol, page 6](#) (required)
- [Verifying the NSF/SSO—MPLS VPN Configuration, page 7](#) (optional)

## Configuring NSF Support for Basic VPNs

Perform this task to configure NSF support for basic VPNs.

### Prerequisites

Route Processors must be configured for SSO. See the [Stateful Switchover](#) feature module for more information.

If you use LDP in the core or in the virtual routing and forwarding (VRF) instances for MPLS VPN Carrier Supporting Carrier configurations, you must enable the MPLS LDP: NSF/SSO Support and Graceful Restart feature. See the [NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart](#) feature module for more information.

You must enable Nonstop Forwarding on the routing protocols running between the P, PE, and CE routers. The routing protocols are OSPF, IS-IS, and BGP. See the [Cisco Nonstop Forwarding](#) feature module for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. Configuration information is included in the [Configuring MPLS VPNs](#) feature module.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **router bgp *as-number***
5. **bgp graceful-restart restart-time *secs***
6. **bgp graceful-restart stalepath-time *secs***
7. **bgp graceful-restart**
8. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables Cisco Express Forwarding <ul style="list-style-type: none"> <li>Use this command if Cisco Express Forwarding is not enabled by default on the router.</li> </ul>
Step 4	<b>router bgp as-number</b>  <b>Example:</b> Router(config)# router bgp 1	Configures a BGP routing process and enters router configuration mode. <ul style="list-style-type: none"> <li>The <i>as-number</i> argument indicates the number of an autonomous system that identifies the router to other BGP routers and tags the routing information passed along.</li> </ul> Valid numbers are from 0 to 65535. Private autonomous system numbers that can be used in internal networks range from 64512 to 65535.
Step 5	<b>bgp graceful-restart restart-time secs</b>  <b>Example:</b> Router(config-router)# bgp graceful-restart restart-time 200	(Optional) Specifies the maximum time to wait for a graceful-restart-capable neighbor to come back up after a restart. The default is 120 seconds. The valid range is from 1 to 3600 seconds.
Step 6	<b>bgp graceful-restart stalepath-time secs</b>  <b>Example:</b> Router(config-router)# bgp graceful-restart stalepath-time 400	(Optional) Specifies the maximum time to hold on to the stale paths of a gracefully restarted peer. All stale paths are deleted after the expiration of this timer. The default is 360 seconds. The valid range is from 1 to 3600 seconds.
Step 7	<b>bgp graceful-restart</b>  <b>Example:</b> Router(config-router)# bgp graceful-restart	Enables BGP Graceful Restart on the router. See <a href="#">Cisco Nonstop Forwarding</a> for more information about the <b>bgp graceful-restart</b> command.
Step 8	<b>end</b>  <b>Example:</b> Router(config-router)# end	(Optional) Exits to privileged EXEC mode.



## Configuring NSF Support for MPLS VPN Interfaces That Use BGP as the Label Distribution Protocol

The following VPN features require special configuration for the NSF/SSO—MPLS VPN feature:

- MPLS VPN—Carrier Supporting Carrier—IPv4 BGP Label Distribution
- MPLS VPN—Inter-AS—IPv4 BGP Label Distribution

You must issue an extra command, **mpls forwarding bgp**, on the interfaces that use BGP to distribute MPLS labels and routes. Use the following procedure to configure the NSF/SSO—MPLS VPN feature in these MPLS VPNs.

### Prerequisites

- Make sure your MPLS VPN is configured for Carrier Supporting Carrier (CSC) or Inter-AS with BGP as the label distribution protocol.
- Configure NSF/SSO—MPLS VPN first, as described in [“Configuring NSF Support for Basic VPNs” section on page 4](#).

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **interface slot/port**
5. **mpls forwarding bgp**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>	Enables privileged EXEC mode.
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>	Enters global configuration mode.
	<b>Example:</b> Router# configure terminal	
Step 3	<b>ip cef [distributed]</b>	Enables Cisco Express Forwarding.
	<b>Example:</b> Router(config)# ip cef distributed	<ul style="list-style-type: none"> <li>• Use this command if Cisco Express Forwarding is not enabled by default on the router.</li> </ul>

	Command or Action	Purpose
Step 4	<code>interface slot/port</code>  <b>Example:</b> Router(config)# interface POS1/0/0	Defines the interface and enters interface configuration mode.
Step 5	<code>mpls forwarding bgp</code>  <b>Example:</b> Router(config-if)# <code>mpls forwarding bgp</code>	Enables the interface to exchange BGP labels. You need to issue this command on any interface configured to use BGP to forward MPLS labels and routes.

## Verifying the NSF/SSO—MPLS VPN Configuration

This section explains how to verify a configuration that has the NSF/SSO—MPLS VPN feature.

- See the [Cisco Nonstop Forwarding](#) feature module for verification procedures for BGP, OSPF, and IS-IS.
- See the [NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart](#) feature module for verification procedures for the MPLS LDP: NSF/SSO feature
- See the verification information included in the [Configuring MPLS VPNs](#) feature module.

### SUMMARY STEPS

1. `show ip bgp vpnv4 all labels`
2. `show ip bgp vpnv4 all neighbors`
3. `show ip bgp labels`
4. `show ip bgp neighbors`

### DETAILED STEPS

#### Step 1 `show ip bgp vpnv4 all labels`

This command displays incoming and outgoing BGP labels for each route distinguisher. The following is sample output from the command:

```
Router# show ip bgp vpnv4 all labels

Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (vpn1)
  10.3.0.0/16      10.0.0.5      25/20
                  10.0.0.1      25/23
                  10.0.0.2      25/imp-null
  10.0.0.9/32      10.0.0.1      24/22
                  10.0.0.2      24/imp-null
```

#### Step 2 `show ip bgp vpnv4 all neighbors`

This command displays whether the BGP peers are capable of Graceful Restart. The following is sample output from the command:

```
Router# show ip bgp vpnv4 all neighbors

BGP neighbor is 10.0.0.1, remote AS 100, internal link
```

```

BGP version 4, remote router ID 10.0.0.1
BGP state = Established, up for 02:49:47
Last read 00:00:47, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family VPNv4 Unicast: advertised and received
  Graceful Restart Capability: advertised and received
    Remote Restart timer is 120 seconds
  Address families preserved by peer:
    VPNv4 Unicast
    .
    .
    .

```

### Step 3 show ip bgp labels

This command displays information about MPLS labels in the Exterior Border Gateway Protocol (EBGP) route table. The following is sample output from the command:

```
Router# show ip bgp labels
```

Network	Next Hop	In label/Out label
10.3.0.0/16	10.0.0.1	imp-null/imp-null
	0.0.0.0	imp-null/nolabel
10.0.0.9/32	10.0.0.1	21/29
10.0.0.11/32	10.0.0.1	24/38
10.0.0.13/32	0.0.0.0	imp-null/nolabel
10.0.0.15/32	10.0.0.1	29/nolabel
	10.0.0.1	29/21

### Step 4 show ip bgp neighbors

This command displays whether the BGP peers are capable of Graceful Restart. The following is sample output from the command:

```
Router# show ip bgp neighbors
```

```

BGP neighbor is 10.0.0.1, remote AS 100, external link
BGP version 4, remote router ID 10.0.0.5
BGP state = Established, up for 02:54:19
Last read 00:00:18, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
  ipv4 MPLS Label capability: advertised and received
  Graceful Restart Capability: advertised and received
    Remote Restart timer is 120 seconds
  Address families preserved by peer:
    IPv4 Unicast
    .
    .
    .

```

## Configuration Examples for NSF/SSO—MPLS VPN

This section includes six configuration examples. The first configuration example shows the most simple configuration, a basic VPN configuration. The second, third, and fourth examples show different CSC VPN configurations. The fourth example shows a CSC VPN configuration that uses BGP as the MPLS label distribution method and therefore requires the **mpls forwarding bgp** command. The last two examples show Inter-AS configurations.

- [NSF/SSO—MPLS VPN for a Basic MPLS VPN: Example, page 9](#)

- [NSF/SSO—MPLS VPN for a CSC Network with a Customer Carrier Who Is an ISP: Example, page 13](#)
- [NSF/SSO—MPLS VPN for a CSC Network with a Customer Who Is an MPLS VPN Provider: Example, page 18](#)
- [NSF/SSO—MPLS VPN for a CSC Network That Uses BGP to Distribute MPLS Labels: Example, page 26](#)
- [NSF/SSO—MPLS VPN for an Inter-AS Network Using BGP to Distribute Routes and MPLS Labels: Example, page 34](#)
- [NSF/SSO—MPLS VPN for an Inter-AS Network That Uses BGP to Distribute Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Example, page 40](#)

## NSF/SSO—MPLS VPN for a Basic MPLS VPN: Example

In this example, the NSF/SSO—MPLS VPN feature is enabled on the existing MPLS VPN configuration.

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the Cisco 7500 series routers:

- `hw-module slot`
- `redundancy`
- `mode sso`

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

### Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

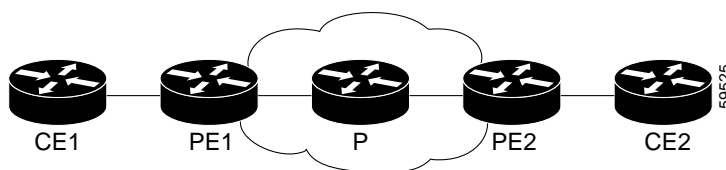
- `bgp graceful-restart restart-time`
- `bgp graceful-restart stalepath-time`
- `bgp graceful-restart`
- `nsf enforce global`



#### Note

In the configuration example, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted by arrows.

[Figure 1](#) shows the configuration of the NSF/SSO—MPLS VPN feature on the PE and CE routers.

**Figure 1** *MPLS VPN Configuration with MPLS VPN: NSF/SSO***Note**

LDP is the default MPLS label protocol.

The following configuration examples show the configuration of the NSF/SSO—MPLS VPN feature on the CE and PE routers.

**CE1 Router**

```
ip cef
no ip domain-lookup
!
interface Loopback0
 ip address 10.10.10.10 255.255.255.255
!
interface Ethernet4
 ip address 10.0.0.1 255.0.0.0
 media-type 10BaseT
!
router ospf 100
 redistribute bgp 101
 nsf enforce global
 passive-interface Ethernet4
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 101
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart network 10.0.0.0
 network 10.0.0.0
 neighbor 10.0.0.2 remote-as 100
```

**PE1 Router**

```
redundancy
 mode sso
!
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp

ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
no mpls aggregate-statistics
!
interface Loopback0
 ip address 10.12.12.12 255.255.255.255
!
interface Ethernet1/4      =====> interface FastEthernet1/1/4 on a Cisco 10000 series router
```

```

ip vrf forwarding vpn1
ip address 10.0.0.2 255.0.0.0
!
mpls ip

interface ATM3/0                                =====> interface ATM3/0/0 on a Cisco 10000 series router
no ip address
!
interface ATM3/0.1 point-to-point ==> interface ATM3/0/0.1 point-to-point on a Cisco 10000
ip unnumbered Loopback0
mpls ip
!
router ospf 100
passive-interface Ethernet1/4    ===> passive-interface FastEthernet1/1/4 on a Cisco 10000
nsf enforce global
network 10.0.0.0 0.255.255.255 area 100
!
router bgp 100
no synchronization
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart

no bgp default ipv4-unicast
neighbor 10.14.14.14 remote-as 100
neighbor 10.14.14.14 update-source Loopback0
!
address-family ipv4 vrf vpn1
neighbor 10.0.0.1 remote-as 101
neighbor 10.0.0.1 activate
exit-address-family
!
address-family vpnv4
neighbor 10.14.14.14 activate
neighbor 10.14.14.14 send-community extended
exit-address-family

```

## PE2 Router

```

redundancy
mode sso
!
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
no mpls aggregate-statistics
!
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
!
interface ATM1/0                                =====> interface ATM1/0/0 on a Cisco 10000 series router
no ip address
!
interface ATM1/0.1 point-to-point ==> interface ATM1/0/0.1 point-to-point on a Cisco 10000
ip unnumbered Loopback0

```

```

mpls ip
!
interface FastEthernet3/0/0
 ip vrf forwarding vpn1
 ip address 10.0.0.1 255.0.0.0
 ip route-cache distributed
 mpls ip
!
router ospf 100
 nsf enforce global
 passive-interface FastEthernet3/0/0
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 100
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 no bgp default ipv4-unicast
 neighbor 10.12.12.12 remote-as 100
 neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4 vrf vpn1
 neighbor 10.0.0.2 remote-as 102
 neighbor 10.0.0.2 activate
 exit-address-family
!
address-family vpnv4
 neighbor 10.12.12.12 activate
 neighbor 10.12.12.12 send-community extended
 exit-address-family

```

## CE2 Router

```

ip cef
!
interface Loopback0
 ip address 10.13.13.13 255.255.255.255
!
interface FastEthernet0
 ip address 10.0.0.2 255.0.0.0
 no ip mroute-cache
!
router ospf 100
 redistribute bgp 102
 nsf enforce global
 passive-interface FastEthernet0
 network 10.0.0.0 0.255.255.255 area 100
!
router bgp 102
 no synchronization
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart

network 10.0.0.0
network 10.0.0.0
neighbor 10.0.0.1 remote-as 100

```

## NSF/SSO—MPLS VPN for a CSC Network with a Customer Carrier Who Is an ISP: Example

In this example, MPLS VPN SSO and NSF are configured on the existing MPLS CSC VPN configuration. In the CSC network configuration, the customer carrier is an Internet Service Provider (ISP), as shown in [Figure 2](#).

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the Cisco 7500 series routers:

- **hw-module slot**
- **redundancy**
- **mode sso**

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

### Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

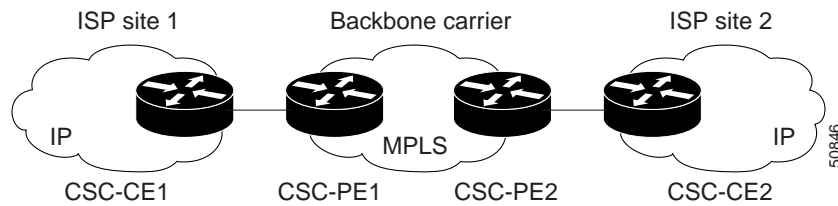
- **bgp graceful-restart restart-time**
- **bgp graceful-restart stalepath-time**
- **bgp graceful-restart**
- **nsf enforce global**



#### Note

In the configuration example, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted by arrows.



**Figure 2** *MPLS VPN CSC Configuration with MPLS VPN: NSF and SSO*

## CSC-CE1 Configuration

```

mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
!
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
!
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
no ip address
!
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
!
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
  nsf enforce global
network 10.14.14.14 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200

```

## CSC-PE1 Configuration

```

redundancy
  mode sso
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!

```

```
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
!
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.19.19.19 255.255.255.255
!
interface ATM1/1/0
no ip address
!
interface ATM1/1/0.1 point-to-point
ip address 10.0.0.1 255.0.0.0
!
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.19.19.19 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart

timers bgp 10 30
neighbor 10.12.12.12 remote-as 100
neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4
```

```

neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-PE2 Configuration

```

redundancy
  mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls ldp graceful-restart
mpls label protocol ldp
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.20.20.20 255.255.255.255
!
interface ATM0/1/0
no ip address
!
interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes

```

```

nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.12.12.12 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.20.20.20 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls label protocol ldp
mpls ldp graceful-restart
!
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM5/0

```

```

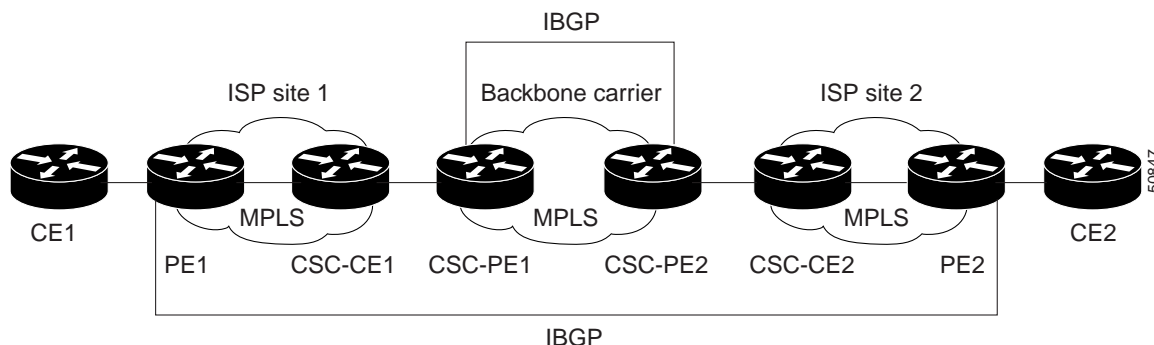
no ip address
!
interface ATM5/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
nsf enforce global
redistribute connected subnets
network 10.16.16.16 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200

```

## NSF/SSO—MPLS VPN for a CSC Network with a Customer Who Is an MPLS VPN Provider: Example

In the CSC network configuration shown in [Figure 3](#), the customer carrier is an MPLS VPN provider. The customer carrier has two sites. The backbone carrier and the customer carrier use MPLS. The internal BGP (iBGP) sessions exchange the external routing information of the ISP.

**Figure 3** *MPLS VPN CSC Configuration 2 with MPLS VPN: NSF and SSO*



The following configuration example shows the configuration of each router in the CSC network. OSPF is the protocol used to connect the customer carrier to the backbone carrier. The NSF/SSO—MPLS VPN feature is enabled on the existing MPLS VPN configuration.

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- `hw-module slot`
- `redundancy`
- `mode sso`

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz

```

```
hw-module slot 3 image slot0:rsp-pv-mz
```

### Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- `bgp graceful-restart restart-time`
- `bgp graceful-restart stalepath-time`
- `bgp graceful-restart`
- `nsf enforce global`



#### Note

In the configuration examples, the NSF/SSO commands are bold-faced and any platform-specific commands are highlighted with arrows.

## CE1 Configuration

```
ip cef
!
interface Loopback0
ip address 10.17.17.17 255.255.255.255
!
interface Ethernet0/1
ip address 10.0.0.2 255.0.0.0
!
router ospf 300
log-adjacency-changes
nsf enforce global
redistribute bgp 300 subnets
passive-interface Ethernet0/1
network 10.17.17.17 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.0.0.1 remote-as 200
neighbor 10.0.0.1 advertisement-interval 5
no auto-summary
```

## PE1 Configuration

```
redundancy
 mode sso
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
```

```

ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
!
interface Loopback0
ip address 10.13.13.13 255.255.255.255
!
interface ATM1/0          =====> interface ATM1/0/0 on a Cisco 10000 series router
no ip address
!
interface ATM1/0.1 point-to-point ===> interface ATM1/0/0 point-to-point on a Cisco 10000
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface Ethernet3/0     =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address 10.0.0.1 255.0.0.0
no ip mroute-cache
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
passive-interface Ethernet3/0 =====> passive-interface FastEthernet3/0/0 on a Cisco 10000

network 10.13.13.13 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.15.15.15 remote-as 200
neighbor 10.15.15.15 update-source Loopback0
!
address-family ipv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.15.15.15 activate
neighbor 10.15.15.15 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 as-override
neighbor 10.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE1 Configuration

```

mpls label protocol ldp
mpls ldp graceful-restart
!
interface Loopback0
ip address 10.14.14.14 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM2/0
no ip address
!
interface ATM2/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
network 10.14.14.14 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200

```

## CSC-PE1 Configuration

```

redundancy
  mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
mpls ldp graceful-restart
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.11.11.11 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.19.19.19 255.255.255.255
!
interface ATM1/1/0

```



```

no ip address
!
interface ATM1/1/0.1 point-to-point
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 101 0 51 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
passive-interface ATM3/0/0.1
nsf enforce global
passive-interface Loopback100
network 10.11.11.11 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.19.19.19 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 10.12.12.12 remote-as 100
neighbor 10.12.12.12 update-source Loopback0
!
address-family ipv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.12.12.12 activate
neighbor 10.12.12.12 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-PE2 Configuration

```

redundancy
  mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:0
route-target export 100:0
route-target import 100:0
mpls label protocol ldp
mpls ldp graceful-restart
no mpls aggregate-statistics
!
interface Loopback0
ip address 10.12.12.12 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface Loopback100
ip vrf forwarding vpn1
ip address 10.20.20.20 255.255.255.255
!
interface ATM0/1/0
no ip address
!
interface ATM0/1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM3/0/0
no ip address
!
interface ATM3/0/0.1 point-to-point
ip vrf forwarding vpn1
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
nsf enforce global
passive-interface ATM3/0/0.1
passive-interface Loopback100
network 10.12.12.12 0.0.0.0 area 100
network 10.0.0.0 0.255.255.255 area 100
!
router ospf 200 vrf vpn1
log-adjacency-changes
nsf enforce global
redistribute bgp 100 metric-type 1 subnets
network 10.20.20.20 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 100
bgp log-neighbor-changes
timers bgp 10 30
bgp graceful-restart restart-time 120

```

```

bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor 10.11.11.11 remote-as 100
neighbor 10.11.11.11 update-source Loopback0
!
address-family ipv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.11.11.11 activate
neighbor 10.11.11.11 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn1
redistribute ospf 200 match internal external 1 external 2
no auto-summary
no synchronization
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.16.16.16 255.255.255.255
no ip route-cache
no ip mroute-cache
!
interface ATM1/0
no ip address
!
interface ATM1/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
interface ATM5/0
no ip address
!
interface ATM5/0.1 point-to-point
ip address 10.0.0.2 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
network 10.16.16.16 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
network 10.0.0.0 0.255.255.255 area 200

```

## PE2 Configuration

```

redundancy
  mode sso
ip cef distributed
ip cef accounting non-recursive
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address 10.15.15.15 255.255.255.255
!
interface Ethernet3/0      =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address 10.0.0.1 255.0.0.0
!
interface ATM5/0           =====> interface ATM5/0/0 on a Cisco 10000 series router
no ip address
!
interface ATM5/0.1 point-to-point ==> interface ATM5/0/0.1 point-to-point on a Cisco 10000
ip address 10.0.0.1 255.0.0.0
atm pvc 100 0 50 aal5snap
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
redistribute connected subnets
nsf enforce global
passive-interface Ethernet3/0  =====> passive-interface FastEthernet3/0/0 on a Cisco 10000
network 10.15.15.15 0.0.0.0 area 200
network 10.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor 10.13.13.13 remote-as 200
neighbor 10.13.13.13 update-source Loopback0
!
address-family ipv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 10.13.13.13 activate
neighbor 10.13.13.13 send-community extended
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor 10.0.0.2 remote-as 300
neighbor 10.0.0.2 activate

```

```
neighbor 10.0.0.2 as-override
neighbor 10.0.0.2 advertisement-interval 5
no auto-summary
no synchronization
exit-address-family
```

## CE2 Configuration

```
ip cef
!
interface Loopback0
ip address 10.18.18.18 255.255.255.255
!
interface Ethernet0/1
ip address 10.0.0.2 255.0.0.0
!
router ospf 300
log-adjacency-changes
nsf enforce global
redistribute bgp 300 subnets
passive-interface Ethernet0/1
network 10.18.18.18 0.0.0.0 area 300
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
redistribute connected
redistribute ospf 300 match internal external 1 external 2
neighbor 10.0.0.1 remote-as 200
neighbor 10.0.0.1 advertisement-interval 5
no auto-summary
```

## NSF/SSO—MPLS VPN for a CSC Network That Uses BGP to Distribute MPLS Labels: Example

In the following example and in [Figure 4](#), the NSF/SSO—MPLS VPN feature is configured on an existing MPLS VPN.

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- `hw-module slot`
- `redundancy`
- `mode sso`

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

### Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- `bgp graceful-restart restart-time`
- `bgp graceful-restart stalepath-time`
- `bgp graceful-restart`
- `nsf enforce global`
- `mpls forwarding bgp`

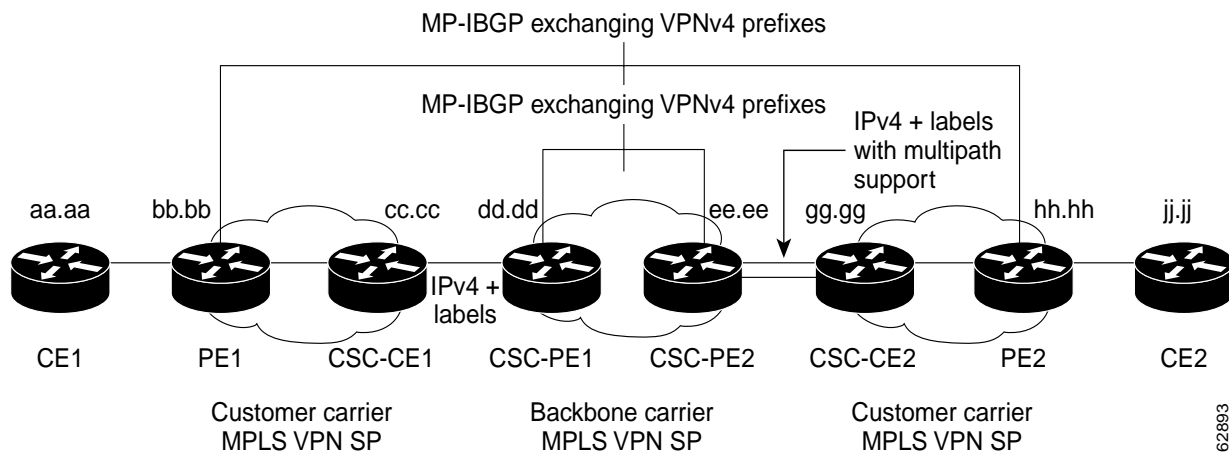


#### Note

In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

This section and [Figure 4](#) provide an example of a backbone carrier and a customer carrier who are both BGP/MPLS VPN service providers. The example shows how BGP is enabled to distribute routes and MPLS labels between PE and CE routers.

**Figure 4** *MPLS VPN CSC Configuration 3 with MPLS VPN: NSF and SSO*



In [Figure 4](#), the subnet mask is 255.255.255.252.

The routers have the following characteristics:

- CE1 and CE2 belong to an end customer. CE1 and CE2 routers exchange routes learned from PE routers. The end customer is purchasing VPN services from a customer carrier.
- PE1 and PE2 are part of a customer carrier network that is configured to provide MPLS VPN services. PE1 and PE2 are peering with a VPNv4 IBGP session to form an MPLS VPN network.
- CSC-CE1 and CSC-CE2 are part of a customer carrier network. CSC-CE1 and CSC-CE2 routers exchange IPv4 BGP updates with MPLS labels and redistribute PE loopback addressees that are sent to and received from the IGP (OSPF in this example). The customer carrier is purchasing Carrier Supporting Carrier VPN services from a backbone carrier.

- CSC-PE1 and CSC-PE2 are part of the backbone carrier's network configured to provide Carrier Supporting Carrier VPN services. CSC-PE1 and CSC-PE2 peer with a VPNv4 IP BGP session to form the MPLS VPN network. In the VRF, CSC-PE1 and CSC-PE2 peer with the CSC-CE routers, which are configured to carry MPLS labels with the routes, within an IPv4 EBGp session.

## CE1 Configuration

```
ip cef
interface Loopback0
ip address aa.aa.aa.aa 255.255.255.255
!
interface Ethernet3/3
ip address mm.0.0.1 255.0.0.0
!
router bgp 300
no synchronization
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
redistribute connected !Exchange routes
neighbor mm.0.0.2 remote-as 200 !learned from PE1.
neighbor mm.0.0.2 advertisement-interval 5
no auto-summary
```

## PE1 Configuration

```
redundancy
  mode sso
ip cef distributed
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address bb.bb.bb.bb 255.255.255.255
!
interface Ethernet3/0      =====> interface FastEthernet3/0/0 on a Cisco 10000 series router
ip address nn.0.0.1 255.0.0.0
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
interface Ethernet3/3      =====> interface FastEthernet3/0/3 on a Cisco 10000 series router
ip vrf forwarding vpn2
ip address mm.0.0.2 255.0.0.0
no ip mroute-cache
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet3/3  ===> passive-interface FastEthernet3/0/3 on a Cisco 10000
network bb.bb.bb.bb 0.0.0.0 area 200
```

```

network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor hh.hh.hh.hh remote-as 200
neighbor hh.hh.hh.hh update-source Loopback0
!
address-family vpnv4 !VPNV4 session with PE2.
neighbor hh.hh.hh.hh activate
neighbor hh.hh.hh.hh send-community extended
bgp dampening 30
exit-address-family
!
address-family ipv4 vrf vpn2
neighbor mm.0.0.1 remote-as 300
neighbor mm.0.0.1 activate
neighbor mm.0.0.1 as-override
neighbor mm.0.0.1 advertisement-interval 5
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## CSC-CE1 Configuration

```

ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address cc.cc.cc.cc 255.255.255.255
!
interface Ethernet3/0
ip address pp.0.0.1 255.0.0.0
mpls forwarding bgp
!
interface Ethernet4/0
ip address nn.0.0.2 255.0.0.0
no ip mroute-cache
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets !Exchange routes
redistribute bgp 200 metric 3 subnets !learned from PE1.
passive-interface ATM1/0
passive-interface Ethernet3/0
network cc.cc.cc.cc 0.0.0.0 area 200
network nn.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes

```



```

bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor pp.0.0.2 remote-as 100
neighbor pp.0.0.2 update-source Ethernet3/0
no auto-summary
!
address-family ipv4
redistribute connected
redistribute ospf 200 metric 4 match internal
neighbor pp.0.0.2 activate
neighbor pp.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## CSC-PE1 Configuration

```

redundancy
  mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
  ip address dd.dd.dd.dd 255.255.255.255
!
interface Ethernet3/1      =====> interface FastEthernet3/0/1 on a Cisco 10000 series router
  ip vrf forwarding vpn1
  ip address pp.0.0.2 255.0.0.0
  mpls forwarding bgp
!
interface ATM0/1/0
  no ip address
!
interface ATM0/1/0.1 point-to-point
  ip unnumbered Loopback0
  no atm enable-ilmi-trap
  mpls label protocol ldp
  mpls ip
!
router ospf 100
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  nsf enforce global
  redistribute connected subnets
  passive-interface Ethernet3/1
  network dd.dd.dd.dd 0.0.0.0 area 100
!
router bgp 100
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart

```

```

timers bgp 10 30
neighbor ee.0.0.0 remote-as 100
neighbor ee.0.0.0 update-source Loopback0
!
address-family vpnv4 !VPNv4 session with CSC-PE2.
neighbor ee.0.0.0 activate
neighbor ee.0.0.0 send-community extended
bgp dampening 30
exit-address-family
!
address-family ipv4 vrf vpn1
neighbor pp.0.0.1 remote-as 200
neighbor pp.0.0.1 activate
neighbor pp.0.0.1 as-override
neighbor pp.0.0.1 advertisement-interval 5
neighbor pp.0.0.1 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## CSC-PE2 Configuration

```

redundancy
mode sso
ip cef distributed
!
ip vrf vpn1
rd 100:1
route-target export 100:1
route-target import 100:1
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address ee.0.0.0 255.255.255.255
!
interface Ethernet5/0 =====> interface FastEthernet5/0/0 on a Cisco 10000 series router
ip vrf forwarding vpn1
ip address ss.0.0.2 255.0.0.0
mpls forwarding bgp
no ip route-cache distributed
clock source internal
!
interface ATM2/1/0
no ip address
!
interface ATM2/1/0.1 point-to-point
ip unnumbered Loopback0
no atm enable-ilmi-trap
mpls label protocol ldp
mpls ip
!
router ospf 100
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet5/0 =====> passive-interface FastEthernet5/0/0 on a Cisco 10000
passive-interface ATM3/0/0
network ee.0.0.0 0.0.0.0 area 100
!

```

```

router bgp 100
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor dd.dd.dd.dd remote-as 100
neighbor dd.dd.dd.dd update-source Loopback0
!
address-family vpnv4 !VPNv4 session with CSC-PE1.
neighbor dd.dd.dd.dd activate
neighbor dd.dd.dd.dd send-community extended
bgp dampening 30
exit-address-family
!
address-family ipv4 vrf vpn1
neighbor ss.0.0.1 remote-as 200
neighbor ss.0.0.1 activate
neighbor ss.0.0.1 as-override
neighbor ss.0.0.1 advertisement-interval 5
neighbor ss.0.0.1 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## CSC-CE2 Configuration

```

ip cef
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
ip address gg.gg.gg.gg 255.255.255.255
!
interface Ethernet2/2
ip address ss.0.0.2 255.0.0.0
no ip mroute-cache
mpls forwarding bgp
!
interface ATM3/1/0.1 point-to-point
ip address yy.0.0.1 255.0.0.0
mpls label protocol ldp
mpls ip
!
router ospf 200
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets !Exchange routes
redistribute bgp 200 metric 3 subnets !learned from PE2.
passive-interface ATM3/1/0.1
network gg.gg.gg.gg 0.0.0.0 area 200
network ss.0.0.0 0.255.255.255 area 200
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360

```

```

bgp graceful-restart
timers bgp 10 30
neighbor yy.0.0.2 remote-as 100
neighbor yy.0.0.2 update-source ATM3/1/0.1
no auto-summary
!
address-family ipv4
redistribute connected
redistribute ospf 200 metric 4 match internal
neighbor yy.0.0.2 activate
neighbor yy.0.0.2 send-label
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## PE2 Configuration

```

redundancy
  mode sso
ip cef distributed
!
ip vrf vpn2
rd 200:1
route-target export 200:1
route-target import 200:1
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
  ip address hh.hh.hh.hh 255.255.255.255
!
interface Ethernet3/6 =====> interface FastEthernet3/0/6 on a Cisco 10000 series router
  ip vrf forwarding vpn2
  ip address tt.0.0.2 255.0.0.0
!
interface ATM5/0.1 point2point
  ip address qq.0.0.1 255.0.0.0
  no atm enable-ilmi-trap
  no ip mroute-cache
  mpls label protocol ldp
  mpls ip
!
router bgp 200
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
!
address-family vpnv4 !VPNV4 session with PE1.
  neighbor bb.bb.bb.bb activate
  neighbor bb.bb.bb.bb send-community extended
  bgp dampening 30
  exit-address-family
!
address-family ipv4 vrf vpn2
  neighbor tt.0.0.1 remote-as 300

```

```

neighbor tt.0.0.1 activate
neighbor tt.0.0.1 as-override
neighbor tt.0.0.1 advertisement-interval 5
no auto-summary
no synchronization
bgp dampening 30
exit-address-family

```

## CE2 Configuration

```

ip cef
!
interface Loopback0
    ip address jj.jj.jj.jj 255.255.255.255
!
interface Ethernet3/6
    ip address tt.0.0.1 255.0.0.0
!
router bgp 300
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
no synchronization
bgp log-neighbor-changes
timers bgp 10 30 !Exchange routes
redistribute connected !learned from PE2.
redistribute ospf 300 match internal external 1 external 2
neighbor tt.0.0.2 remote-as 200
neighbor tt.0.0.2 advertisement-interval 5
no auto-summary

```

## NSF/SSO—MPLS VPN for an Inter-AS Network Using BGP to Distribute Routes and MPLS Labels: Example

In [Figure 5](#) and in the following example, the NSF/SSO—MPLS VPN feature is configured on the existing MPLS VPN Inter-AS configuration.

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- hw-module slot
- redundancy
- mode sso

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```

boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz

```

### Enabling SSO on a Cisco 10000 Series Router

The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- `bgp graceful-restart restart-time`
- `bgp graceful-restart stalepath-time`
- `bgp graceful-restart`
- `nsf enforce global`
- `mpls forwarding bgp`

Inter-AS with IPv4 BGP Label Distribution enables you to set up a VPN so that the ASBRs exchange IPv4 routes with MPLS labels of the PE routers. Route reflectors (RRs) exchange VPNv4 routes by using Multihop, Multiprotocol EBGP. This configuration saves the ASBRs from having to store all of the VPNv4 routes. Using the RRs to store the VPNv4 routes and forward them to the PE routers improves scalability.

Figure 5 shows two MPLS VPN service providers. They distribute VPNv4 addresses between the RRs and IPv4 routes and MPLS labels between ASBRs.

**Figure 5** *MPLS VPN Inter-AS Configuration with MPLS VPN: NSF/SSO*

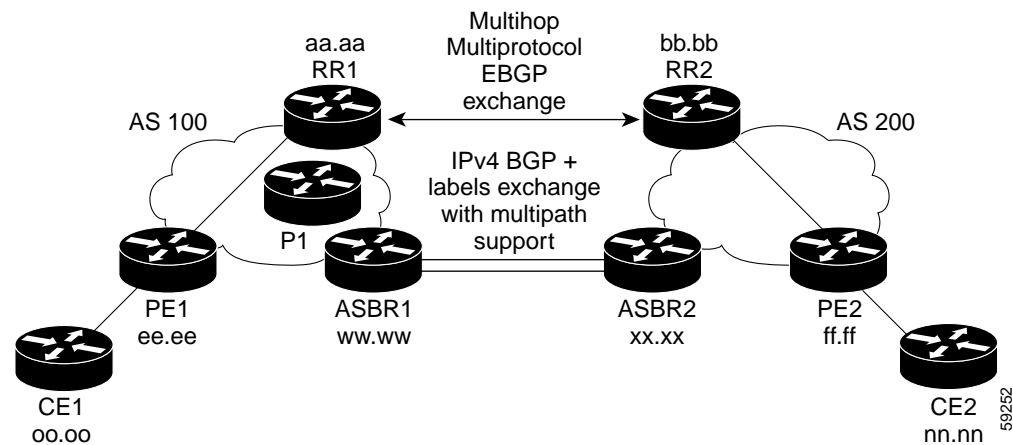


Figure 5 shows the two techniques you can use to distribute the VPNv4 routes and the IPv4 routes and MPLS labels of remote PEs and RRs to local PEs and RRs:

- AS 100 uses the route reflectors to distribute the IPv4 routes and MPLS labels and the VPNv4 routes from the ASBR to the PE.
- In AS 200, the IPv4 routes that ASBR2 learned are redistributed into IGP.



#### Note

In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

## RR1 Configuration

The configuration example for RR1 specifies the following:

- RR1 exchanges VPNv4 routes with RR2, using Multihop, Multiprotocol EBGP.

- The VPNv4 next hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1 the VPNv4 routes learned from RR2 and the IPv4 routes and MPLS labels learned from ASBR1.

```

redundancy
  mode sso
ip subnet-zero
ip cef distributed

!
interface Loopback0
  ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
  ip address dd.0.0.2 255.0.0.0
  clockrate 124061
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
network aa.aa.aa.aa 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor ee.aa.aa.aa remote-as 100
neighbor ee.aa.aa.aa update-source Loopback0
neighbor ww.ww.ww.ww remote-as 100
neighbor ww.ww.ww.ww update-source Loopback0
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb ebgp-multihop 255
neighbor bb.bb.bb.bb update-source Loopback0
no auto-summary
!
address-family ipv4
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa route-reflector-client !IPv4+labels session to PE1
  neighbor ee.aa.aa.aa send-label
  neighbor ww.ww.ww.ww activate
  neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
  neighbor ww.ww.ww.ww send-label
  no neighbor bb.bb.bb.bb activate
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor ee.aa.aa.aa activate
  neighbor ee.aa.aa.aa route-reflector-client !VPNv4 session with PE1
  neighbor ee.aa.aa.aa send-community extended
  neighbor bb.bb.bb.bb activate
  neighbor bb.bb.bb.bb next-hop-unchanged
  !MH-VPNv4 session with RR2 with next hop unchanged
  neighbor bb.bb.bb.bb send-community extended
  exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless

```

=====> Serial1/0/2 on a Cisco 10000 series router

```
!
end
```

## ASBR1 Configuration

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

```
redundancy
  mode sso
ip cef distributed
ip subnet-zero
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
  ip address ww.ww.ww.ww 255.255.255.255
  no ip route-cache
  no ip mroute-cache
!
interface Ethernet0/2      =====> interface FastEthernet1/0/2 on a Cisco 10000 series router
  ip address hh.0.0.2 255.0.0.0
  no ip mroute-cache
  mpls forwarding bgp
!
interface Ethernet0/3      =====> interface FastEthernet1/0/3 on a Cisco 10000 series router
  ip address dd.0.0.1 255.0.0.0
  no ip mroute-cache
  mpls label protocol ldp
  mpls ip
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
passive-interface Ethernet0/2 =====> passive-interface FastEthernet1/0/2 on a Cisco 10000
network ww.ww.ww.ww 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa update-source Loopback0
neighbor hh.0.0.1 remote-as 200
no auto-summary
! Redistributing IGP into BGP
! so that PE1 & RR1 loopbacks
! get into the BGP table.
address-family ipv4
redistribute ospf 10
neighbor aa.aa.aa.aa activate
neighbor aa.aa.aa.aa send-label
neighbor hh.0.0.1 activate
neighbor hh.0.0.1 advertisement-interval 5
neighbor hh.0.0.1 send-label
no auto-summary
no synchronization
exit-address-family
!
```



```
ip default-gateway 10.3.0.1
ip classless
end
```

## RR2 Configuration

RR2 exchanges VPNv4 routes with RR1 through Multihop, Multiprotocol EBGP. In this configuration, the next hop information and the VPN label are preserved across the autonomous systems.

```
ip subnet-zero
ip cef
!
interface Loopback0
    ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
    ip address ii.0.0.2 255.0.0.0
    no ip mroute-cache
!
router ospf 20
log-adjacency-changes
network bb.bb.bb.bb 0.0.0.0 area 200
network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp cluster-id 1
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa ebgp-multihop 255
neighbor aa.aa.aa.aa update-source Loopback0
neighbor ff.ff.ff.ff remote-as 200
neighbor ff.ff.ff.ff update-source Loopback0
no auto-summary
!
address-family vpnv4
    neighbor aa.aa.aa.aa activate
    neighbor aa.aa.aa.aa next-hop-unchanged
    !Multihop VPNv4 session with RR1 with next-hop unchanged
    neighbor aa.aa.aa.aa send-community extended
    neighbor ff.ff.ff.ff activate
    neighbor ff.ff.ff.ff route-reflector-client !VPNv4 session with PE2
    neighbor ff.ff.ff.ff send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
end
```

## ASBR2 Configuration

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can reach these prefixes.

```
ip subnet-zero
ip cef
```

```

!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
    ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet1/0
    ip address hh.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls forwarding bgp
!
interface Ethernet1/2
    ip address jj.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 20
log-adjacency-changes
auto-cost reference-bandwidth 1000
nsf enforce global
redistribute connected subnets
redistribute bgp 200 subnets
passive-interface Ethernet1/0
! redistributing the routes learned from ASBR1
!(EBGP+labels session) into IGP so that PE2
! will learn them
network xx.xx.xx.xx 0.0.0.0 area 200
network jj..0.0 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
neighbor hh.0.0.2 remote-as 100
no auto-summary
!
address-family ipv4
    redistribute ospf 20
    ! Redistributing IGP into BGP
    ! so that PE2 & RR2 loopbacks
    ! will get into the BGP-4 table
    neighbor hh.0.0.2 activate
    neighbor hh.0.0.2 advertisement-interval 5
    neighbor hh.0.0.2 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
address-family vpnv4
    neighbor bb.bb.bb.bb activate
    neighbor bb.bb.bb.bb send-community extended
    exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end

```

## NSF/SSO—MPLS VPN for an Inter-AS Network That Uses BGP to Distribute Routes and MPLS Labels over a Non-MPLS VPN Service Provider: Example

In this example, the NSF/SSO—MPLS VPN feature is configured on an existing MPLS VPN.

### Enabling SSO on a Cisco 7500 Series Router

The following commands are used to enable SSO on the routers:

- `hw-module slot`
- `redundancy`
- `mode sso`

The configuration examples are the same for both platforms with the exception that the following configuration boot commands are seen in the beginning of a Cisco 7500 series router configuration (and not in a Cisco 10000 series router configuration):

```
boot system slot0:rsp-pv-mz
hw-module slot 2 image slot0:rsp-pv-mz
hw-module slot 3 image slot0:rsp-pv-mz
```

### Enabling SSO on a Cisco 10000 Series Router

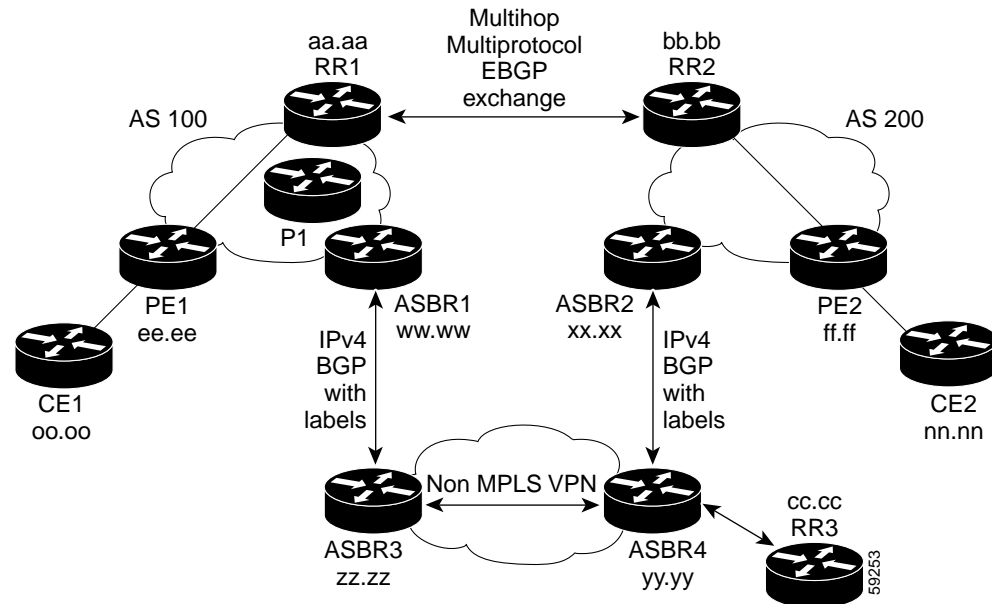
The SSO mode is enabled by default.

### Enabling NSF on Both the Cisco 7500 Series and Cisco 10000 Series Routers

The following commands are used to enable NSF for the routing protocols, such as BGP and OSPF, and for the label distribution protocols, such as BGP and LDP:

- `bgp graceful-restart restart-time`
- `bgp graceful-restart stalepath-time`
- `bgp graceful-restart`
- `nsf enforce global`
- `mpls forwarding bgp`

[Figure 6](#) shows two MPLS VPN service providers that are connected through a non-MPLS VPN service provider. The autonomous system in the middle of the network is configured as a backbone autonomous system that uses LDP to distribute MPLS labels. You can also use traffic engineering tunnels instead of LDP to build the LSP across the non-MPLS VPN service provider.

**Figure 6** *MPLS VPN Inter-AS Configuration 2 with MPLS VPN: NSF/SSO***Note**

In the configuration examples, the NSF/SSO commands are bold-faced and arrows highlight any platform-specific commands.

## RR1 Configuration

The configuration example for RR1 specifies the following:

- RR1 exchanges VPNv4 routes with RR2, using Multihop, Multiprotocol EBGP.
- The VPNv4 next hop information and the VPN label are preserved across the autonomous systems.
- RR1 reflects to PE1 the VPNv4 routes learned from RR2 and the IPv4 routes and MPLS labels learned from ASBR1.

```
ip subnet-zero
ip cef
!
interface Loopback0
  ip address aa.aa.aa.aa 255.255.255.255
!
interface Serial1/2
  ip address dd.0.0.2 255.0.0.0
  clockrate 124061
!
router ospf 10
log-adjacency-changes
auto-cost reference-bandwidth 1000
network aa.aa.aa.aa 0.0.0.0 area 100
network dd.dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
  bgp cluster-id 1
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
```

```

timers bgp 10 30
neighbor ee.ee.ee.ee remote-as 100
neighbor ee.ee.ee.ee update-source Loopback0
neighbor ww.ww.ww.ww remote-as 100
neighbor ww.ww.ww.ww update-source Loopback0
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb ebgp-multihop 255
neighbor bb.bb.bb.bb update-source Loopback0
no auto-summary
!
address-family ipv4
  neighbor ee.ee.ee.ee activate
  neighbor ee.ee.ee.ee route-reflector-client !IPv4+labels session to PE1
  neighbor ee.ee.ee.ee send-label
  neighbor ww.ww.ww.ww activate
  neighbor ww.ww.ww.ww route-reflector-client !IPv4+labels session to ASBR1
  neighbor ww.ww.ww.ww send-label
  no neighbor bb.bb.bb.bb activate
  no auto-summary
  no synchronization
  exit-address-family
!
address-family vpnv4
  neighbor ee.ee.ee.ee activate
  neighbor ee.ee.ee.ee route-reflector-client !VPNv4 session with PE1
  neighbor ee.ee.ee.ee send-community extended
  neighbor bb.bb.bb.bb activate
  neighbor bb.bb.bb.bb next-hop-unchanged
  !MH-VPNv4 session with RR2 with next-hop-unchanged
  neighbor bb.bb.bb.bb send-community extended
  exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
!
snmp-server engineID local 00000009020000D0584B25C0
snmp-server community public RO
snmp-server community write RW
no snmp-server ifindex persist
snmp-server packetsize 2048
!
end

```

## ASBR1 Configuration

ASBR1 exchanges IPv4 routes and MPLS labels with ASBR2.

```

redundancy
  mode sso

ip subnet-zero
ip cef distributed
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
  ip address ww.ww.ww.ww 255.255.255.255
  no ip route-cache
  no ip mroute-cache
!
interface Serial3/0/0
  ip address kk.0.0.2 255.0.0.0
  mpls forwarding bgp

```

```

        ip route-cache distributed
    !
interface Ethernet0/3
    ip address dd.0.0.1 255.0.0.0
    no ip mroute-cache
    mpls label protocol ldp
    mpls ip
!
router ospf 10
log-adjacency-changes
nsf enforce global
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Serial3/0/0
network ww.ww.ww.ww 0.0.0.0 area 100
network dd.0.0.0 0.255.255.255 area 100
!
router bgp 100
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor aa.aa.aa.aa remote-as 100
neighbor aa.aa.aa.aa update-source Loopback0
neighbor kk.0.0.1 remote-as 200
no auto-summary
!
address-family ipv4
    redistribute ospf 10 ! Redistributing IGP into BGP
    neighbor aa.aa.aa.aa activate ! so that PE1 & RR1 loopbacks
    neighbor aa.aa.aa.aa send-label ! get into BGP table
    neighbor kk.0.0.1 activate
    neighbor kk.0.0.1 advertisement-interval 5
    neighbor kk.0.0.1 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end

```

## RR2 Configuration

RR2 exchanges VPNv4 routes with RR1, using Multihop, Multiprotocol EBGp. This configuration also preserves the next hop information and the VPN label across the autonomous systems.

```

ip subnet-zero
ip cef
!
interface Loopback0
    ip address bb.bb.bb.bb 255.255.255.255
!
interface Serial1/1
    ip address ii.0.0.2 255.0.0.0
    no ip mroute-cache
!
router ospf 20
log-adjacency-changes
network bb.bb.bb.bb 0.0.0.0 area 200

```

```

network ii.0.0.0 0.255.255.255 area 200
!
router bgp 200
  bgp cluster-id 1
  bgp log-neighbor-changes
  bgp graceful-restart restart-time 120
  bgp graceful-restart stalepath-time 360
  bgp graceful-restart
  timers bgp 10 30
  neighbor aa.aa.aa.aa remote-as 100
  neighbor aa.aa.aa.aa ebgp-multihop 255
  neighbor aa.aa.aa.aa update-source Loopback0
  neighbor ff.ff.ff.ff remote-as 200
  neighbor ff.ff.ff.ff update-source Loopback0
  no auto-summary
!
address-family vpnv4
  neighbor aa.aa.aa.aa activate
  neighbor aa.aa.aa.aa next-hop-unchanged
  !MH Vpnv4 session with RR1 with next-hop-unchanged
  neighbor aa.aa.aa.aa send-community extended
  neighbor ff.ff.ff.ff activate
  neighbor ff.ff.ff.ff route-reflector-client !Vpnv4 session with PE2
  neighbor ff.ff.ff.ff send-community extended
  exit-address-family
!
ip default-gateway 10.3.0.1
no ip classless
!
end

```

## ASBR2 Configuration

ASBR2 exchanges IPv4 routes and MPLS labels with ASBR1. However, in contrast to ASBR1, ASBR2 does not use the RR to reflect IPv4 routes and MPLS labels to PE2. Instead, ASBR2 redistributes the IPv4 routes and MPLS labels learned from ASBR1 into IGP. PE2 can now reach these prefixes.

```

redundancy
  mode sso
ip subnet-zero
ip cef distributed
!
mpls ldp graceful-restart
mpls label protocol ldp
!
interface Loopback0
  ip address xx.xx.xx.xx 255.255.255.255
!
interface Ethernet0/1 =====> interface FastEthernet1/0/1 on a Cisco 10000 series router
  ip address qq.0.0.2 255.0.0.0
  mpls forwarding bgp
!
interface Ethernet1/2 =====> interface FastEthernet1/1/2 on a Cisco 10000 series router
  ip address jj.0.0.1 255.0.0.0
  no ip mroute-cache
  mpls label protocol ldp
  mpls ip
!
router ospf 20
  log-adjacency-changes
  auto-cost reference-bandwidth 1000
  nsf enforce global

```

```

redistribute connected subnets
redistribute bgp 200 subnets
!redistributing the routes learned from ASBR4
!(EBGP+labels session) into IGP so that PE2
!will learn them
passive-interface Ethernet0/1      =====> passive-interface FastEthernet1/0/1 on a Cisco 10000
network xx.xx.xx.xx 0.0.0.0 area 200
network jj.0.0.0 0.255.255.255 area 200
!
router bgp 200
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor bb.bb.bb.bb remote-as 200
neighbor bb.bb.bb.bb update-source Loopback0
neighbor qq.0.0.1 remote-as 100
no auto-summary
!
address-family ipv4
! Redistributing IGP into BGP redistribute ospf 20
! so that PE2 & RR2 loopbacks
! will get into the BGP-4 table
neighbor qq.0.0.1 activate
neighbor qq.0.0.1 advertisement-interval 5
neighbor qq.0.0.1 send-label
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor bb.bb.bb.bb activate
neighbor bb.bb.bb.bb send-community extended
exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end

```

## ASBR3 Configuration

ASBR3 belongs to a non-MPLS VPN service provider. ASBR3 exchanges IPv4 routes and MPLS labels with ASBR1. ASBR3 also passes the routes learned from ASBR1 to ASBR3 through RR3.



### Note

Do not redistribute EBGP routes learned into internal BGP if you are using IBGP to distribute the routes and labels. This is not a supported configuration.

```

ip subnet-zero
ip cef
!
interface Loopback0
    ip address yy.yy.yy.yy 255.255.255.255
    no ip route-cache
    no ip mroute-cache
!
interface Hssi4/0
    ip address mm.0.0.0.1 255.0.0.0
    no ip mroute-cache

```

=====> only on a Cisco 7500 series router  
=====> only on a Cisco 7500 series router  
=====> only on a Cisco 7500 series router



```

mpls ip                      =====> only on a Cisco 7500 series router
hssi internal-clock          =====> only on a Cisco 7500 series router
!
interface Serial5/0          =====> Serial5/0/0 on a Cisco 10000 series router
 ip address kk.0.0.1 255.0.0.0
 no ip mroute-cache
 load-interval 30
 clockrate 124061
 mpls forwarding bgp
!
router ospf 30
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 redistribute connected subnets
 network yy.yy.yy.yy 0.0.0.0 area 300
 network mm.0.0.0 0.255.255.255 area 300  =====> only on a Cisco 7500 series router
!
router bgp 300
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 timers bgp 10 30
 neighbor cc.cc.cc.cc remote-as 300
 neighbor cc.cc.cc.cc update-source Loopback0
 neighbor kk.0.0.2 remote-as 100
 no auto-summary
!
address-family ipv4
 neighbor cc.cc.cc.cc activate ! IBGP+labels session with RR3
 neighbor cc.cc.cc.cc send-label
 neighbor kk.0.0.2 activate ! EBGP+labels session with ASBR1
 neighbor kk.0.0.2 advertisement-interval 5
 neighbor kk.0.0.2 send-label
 no auto-summary
 no synchronization
 exit-address-family
!
end

```

## RR3 Configuration

RR3 is a non-MPLS VPN RR that reflects IPv4 routes with MPLS labels to ASBR3 and ASBR4.

```

ip subnet-zero
!
interface Loopback0
 ip address cc.cc.cc.cc 255.255.255.255
!
interface POS0/2             =====> interface POS1/0/2 on a Cisco 10000 series router
 ip address pp.0.0.1 255.0.0.0
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 crc 16
 clock source internal
!
router ospf 30
 log-adjacency-changes
 network cc.cc.cc.cc 0.0.0.0 area 300
 network pp.0.0.0 0.255.255.255 area 300
!
router bgp 300

```

```

bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
neighbor zz.zz.zz.zz remote-as 300
neighbor zz.zz.zz.zz update-source Loopback0
neighbor yy.yy.yy.yy remote-as 300
neighbor yy.yy.yy.yy update-source Loopback0
no auto-summary
!
address-family ipv4
  neighbor zz.zz.zz.zz activate
  neighbor zz.zz.zz.zz route-reflector-client
  neighbor zz.zz.zz.zz send-label ! IBGP+labels session with ASBR3
  neighbor yy.yy.yy.yy activate
  neighbor yy.yy.yy.yy route-reflector-client
  neighbor yy.yy.yy.yy send-label ! IBGP+labels session with ASBR4
  no auto-summary
  no synchronization
  exit-address-family
!
ip default-gateway 10.3.0.1
ip classless
!
end

```

## ASBR4 Configuration

ASBR4 belongs to a non-MPLS VPN service provider. ASBR4 and ASBR3 exchange IPv4 routes and MPLS labels by means of RR3.



### Note

If you use IBGP to distribute the routes and labels, do not redistribute EBGP learned routes into IBGP. This is not a supported configuration.

```

redundancy
  mode sso
mpls ldp graceful-restart
ip subnet-zero
ip cef distributed
!
interface Loopback0
  ip address zz.zz.zz.zz 255.255.255.255
  no ip route-cache
  no ip mroute-cache
!
interface Ethernet0/2      =====> interface FastEthernet1/0/2 on a Cisco 10000 series router
  ip address qq.0.0.1 255.0.0.0
  no ip mroute-cache
  mpls forwarding bgp
!
interface POS1/1/0
  ip address pp.0.0.2 255.0.0.0
  ip route-cache distributed
!
interface Hssi2/1/1
  ip address mm.0.0.2 255.0.0.0      =====> only on a Cisco 7500 series router
  ip route-cache distributed        =====> only on a Cisco 7500 series router
  no ip mroute-cache               =====> only on a Cisco 7500 series router
  mpls label protocol ldp          =====> only on a Cisco 7500 series router
  mpls ip                         =====> only on a Cisco 7500 series router

```

```

    hssi internal-clock          =====> only on a Cisco 7500 series router
!
router ospf 30
log-adjacency-changes
nsf enforce global
auto-cost reference-bandwidth 1000
redistribute connected subnets
passive-interface Ethernet0/2   =====> passive-interface FastEthernet1/0/2 on a Cisco 10000
network zz.zz.zz.zz 0.0.0.0 area 300
network pp.0.0.0 0.255.255.255 area 300
network mm.0.0.0 0.255.255.255 area 300
!
router bgp 300
bgp log-neighbor-changes
bgp graceful-restart restart-time 120
bgp graceful-restart stalepath-time 360
bgp graceful-restart
timers bgp 10 30
neighbor cc.cc.cc.cc remote-as 300
neighbor cc.cc.cc.cc update-source Loopback0
neighbor qq.0.0.2 remote-as 200
no auto-summary
!
address-family ipv4
    neighbor cc.cc.cc.cc activate
    neighbor cc.cc.cc.cc send-label
    neighbor qq.0.0.2 activate
    neighbor qq.0.0.2 advertisement-interval 5
    neighbor qq.0.0.2 send-label
    no auto-summary
    no synchronization
    exit-address-family
!
ip classless
end

```

# Additional References

The following sections provide additional information related to the NSF/SSO—MPLS VPN feature.

## Related Documents

Related Topic	Document Title
Nonstop forwarding and BGP Graceful Restart	<a href="#">Cisco Nonstop Forwarding</a>
Nonstop forwarding for MPLS LDP	<a href="#">NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart</a>
Stateful switchover	<a href="#">Stateful Switchover</a>
Basic VPNs, MPLS VPN interautonomous systems, MPLS VPN Carrier Supporting Carrier	<a href="#">Configuring MPLS VPNs</a>

## Standards

Standards	Title
draft-ietf-mpls-bgp-mpls-restart.txt	Graceful Restart Mechanism for BGP with MPLS
draft-ietf-mpls-idr-restart.txt	Graceful Restart Mechanism for BGP

## MIBs

MIBs	MIBs Link
MPLS VPN MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 1163	A Border Gateway Protocol
RFC 1164	Application of the Border Gateway Protocol in the Internet
RFC 2283	Multiprotocol Extensions for BGP-4
RFC 2547	BGP/MPLS VPNs

## Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **mpls forwarding bgp**
- **show ip bgp labels**
- **show ip bgp vpv4**

# Feature Information for NSF/SSO—MPLS VPN

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for NSF/SSO—MPLS VPN

Feature Name	Releases	Feature Information
NSF/SSO—MPLS VPN	12.2(25)S 12.2(28)SB 12.2(33)SRA 12.2(33)SXH	<p>This feature allows a provider edge (PE) router or Autonomous System Border Router (ASBR) (with redundant Route Processors) to preserve data forwarding information in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) when the primary Route Processor restarts.</p> <p>In 12.2(25)S, this feature was introduced on the Cisco 7500 series router.</p> <p>In 12.2(28)SB, support was added for the Cisco 10000 series routers.</p> <p>In 12.2(33)SRA, support was added for the Cisco 7600 series routers.</p> <p>In 12.2(33)SXH, this feature was integrated into this release.</p>

---

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2008 Cisco Systems, Inc. All rights reserved.

---



# AToM Graceful Restart

---

**First Published: August 9, 2004**

**Last Updated: February 27, 2009**

The AToM Graceful Restart feature assists neighboring routers that have nonstop forwarding (NSF), stateful switchover (SSO) and graceful restart (GR) for Any Transport over MPLS (AToM) to recover gracefully from an interruption in service. AToM GR functions strictly in helper mode, which means it helps other routers that are enabled with the NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature to recover. If the router with AToM GR fails, its peers cannot help it recover. AToM GR is based on the MPLS Label Distribution Protocol (LDP) Graceful Restart feature.

Keep the following points in mind when reading this document:

- The AToM GR feature described in this document refers to helper mode.
- The NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature is supported in Cisco IOS Releases 12.2(25)S and 12.2(33)SRA. For brevity, the NSF/SSO: Any Transport over MPLS and AToM Graceful Restart feature is called AToM SSO/NSF in this document.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for AToM Graceful Restart” section on page 8](#).

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

## Contents

- [Information About AToM Graceful Restart, page 2](#)
- [How to Configure AToM Graceful Restart, page 2](#)



---

**Americas Headquarters:**

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



- [Configuration Examples for AToM Graceful Restart, page 3](#)
- [Additional References, page 6](#)
- [Command Reference, page 7](#)
- [Feature Information for AToM Graceful Restart, page 8](#)

## Information About AToM Graceful Restart

To configure AToM GR, you should understand the following concepts:

- [How AToM Graceful Restart Works, page 2](#)

## How AToM Graceful Restart Works

AToM GR works in strict helper mode, which means it helps a neighboring route processor that has AToM NSF/SSO to recover from a disruption in service without losing its MPLS forwarding state. The disruption in service could result from a TCP or User Datagram Protocol (UDP) event or the stateful switchover of a route processor. AToM GR is based on the MPLS LDP Graceful Restart feature, which preserves forwarding information for AToM circuits during an LDP session interruption. When the neighboring router establishes a new session, the LDP bindings and MPLS forwarding state are recovered. For more information related to how the LDP Graceful Restart feature works, see the [MPLS LDP Graceful Restart](#) feature module.

## How to Configure AToM Graceful Restart

This section contains the following procedures:

- [Configuring AToM Graceful Restart, page 2](#) (required)

## Configuring AToM Graceful Restart

There is no AToM-specific configuration for AToM GR. You enable LDP GR to assist a neighboring router configured with AToM NSF/SSO to maintain its forwarding state while the LDP session is disrupted.

### Prerequisites

- See the [MPLS LDP Graceful Restart](#) document for information about how LDP GR works and how you can customize it for your network.
- Configure AToM. For information about setting up or configuring AToM, see the [Any Transport over MPLS](#) document.

### Restrictions

- AToM GR is supported in strict helper mode.
- AToM NSF/SSO is supported in Cisco IOS Release 12.2(25)S and 12.2(33)SRA.

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS LDP GR cannot be configured on label-controlled ATM (LC-ATM) interfaces.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp graceful-restart**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables Cisco Express Forwarding.
Step 4	<b>mpls ldp graceful-restart</b>  <b>Example:</b> Router(config)# mpls ldp graceful-restart	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.  AToM GR is enabled globally. When you enable AToM GR, it has no effect on existing LDP sessions. New LDP sessions that are established can perform AToM GR.

# Configuration Examples for AToM Graceful Restart

This section provides the following configuration examples:

- [AToM Graceful Restart: Configuration Example, page 4](#)
- [AToM Graceful Restart: Recovering from an LDP Session Disruption Example, page 4](#)

## AToM Graceful Restart: Configuration Example

The following example shows an Ethernet VLAN over MPLS configuration. PE1 is configured with AToM Graceful Restart. PE2 is configured with AToM NSF/SSO. The commands for configuring AToM GR and NSF/SSO are shown in bold.

PE1 with AToM GR	PE2 with AToM NSF/SSO
<pre> ip cef ! mpls label protocol ldp <b>mpls ldp graceful-restart</b> mpls ldp router-id Loopback0 ! pseudowire-class atom encapsulation mpls ! interface Loopback0  ip address 10.1.1.2 255.255.255.255 ! interface FastEthernet5/1/1  no ip address ! interface FastEthernet5/1/1.2  description "xconnect to PE2"  encapsulation dot1q 2 native  xconnect 10.2.2.2 1002 pw-class mpls ! ! IGP for MPLS router ospf 10  log-adjacency-changes  auto-cost reference-bandwidth 1000  network 10.1.1.2 10.0.0.0 area 0  network 10.1.1.0 10.0.0.255 area 0 </pre>	<pre> <b>redundancy</b>   <b>mode sso</b> ip cef ! mpls label protocol ldp <b>mpls ldp graceful-restart</b> mpls ldp router-id Loopback0 ! pseudowire-class atom encapsulation mpls ! interface Loopback0  ip address 10.2.2.2 255.255.255.255 ! interface Ethernet3/3  no ip address ! interface Ethernet3/3.2  description "xconnect to PE1"  encapsulation dot1q 2  xconnect 10.1.1.2 1002 pw-class mpls ! ! IGP for MPLS router ospf 10  log-adjacency-changes <b>nsf enforce global</b>  auto-cost reference-bandwidth 1000  network 10.2.2.2 10.0.0.0 area 0  network 10.1.1.0 10.0.0.255 area 0 </pre>

## AToM Graceful Restart: Recovering from an LDP Session Disruption Example

The following examples show the output of the **show mpls l2transport vc** command during normal operation and when an LDP session is recovering from a disruption.

The following example shows the status of the VC on PE1 with AToM GR during normal operation:

Router# **show mpls l2transport vc**

Local intf	Local circuit	Dest address	VC ID	Status
Fa5/1/1.2	Eth VLAN 2	10.2.2.2	1002	UP

The following example shows the status of the VC on PE1 with AToM GR while the VC is recovering from an LDP session disruption. The forwarding state for the circuit remains as it was before the disruption.

Router# **show mpls l2transport vc**

Local intf	Local circuit	Dest address	VC ID	Status
Fa5/1/1.2	Eth VLAN 2	10.2.2.2	1002	RECOVERING

The following example shows the status of the VC on PE1 with AToM GR after the LDP session disruption was cleared. The AToM label bindings were advertised within the allotted time and the status returned to UP.

```
Router# show mpls l2transport vc
```

Local intf	Local circuit	Dest address	VC ID	Status
Fa5/1/1.2	Eth VLAN 2	10.2.2.2	1002	UP

The following example shows the detailed status of the VC on PE1 with AToM GR during normal operation:

```
Router# show mpls l2transport vc detail
```

```
Local interface: Fa5/1/1.2 up, line protocol up, Eth VLAN 2 up
  Destination address: 10.2.2.2, VC ID: 1002, VC status: up
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
    Output interface: Se4/0/3, imposed label stack {16}
  Create time: 1d00h, last status change time: 1d00h
  Signaling protocol: LDP, peer 10.2.2.2:0 up
    MPLS VC labels: local 21, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: "xconnect to PE2"
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 3466, send 12286
    byte totals:   receive 4322368, send 5040220
    packet drops:  receive 0, send 0
```

The following example shows the detailed status of the VC on PE1 with AToM GR while the VC is recovering.

```
Router# show mpls l2transport vc detail
```

```
Local interface: Fa5/1/1.2 up, line protocol up, Eth VLAN 2 up
  Destination address: 10.2.2.2, VC ID: 1002, VC status: recovering
    Preferred path: not configured
    Default path: active
    Tunnel label: imp-null, next hop point2point
    Output interface: Se4/0/3, imposed label stack {16}
  Create time: 1d00h, last status change time: 00:00:03
  Signaling protocol: LDP, peer 10.2.2.2:0 down
    MPLS VC labels: local 21, remote 16
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: "xconnect to PE2"
  Sequencing: receive disabled, send disabled
  VC statistics:
    packet totals: receive 20040, send 28879
    byte totals:   receive 25073016, send 25992388
    packet drops:  receive 0, send 0
```

# Additional References

The following sections provide references related to AToM GR.

## Related Documents

Related Topic	Document Title
MPLS LDP graceful restart	<i><a href="#">MPLS LDP Graceful Restart</a></i>
Configuring AToM	<i><a href="#">Any Transport over MPLS</a></i>
Nonstop forwarding and stateful switchover for AToM	<i><a href="#">NSF/SSO—Any Transport over MPLS and AToM Graceful Restart</a></i>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 3036	<i><a href="#">LDP Specification</a></i>
RFC 3478	<i><a href="#">Graceful Restart Mechanism for Label Distribution</a></i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

This feature uses no new or modified commands.

# Feature Information for AToM Graceful Restart

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for AToM Graceful Restart

Feature Name	Releases	Feature Information
AToM Graceful Restart	12.0(29)S	In 12.0(29)S, this feature was introduced.
	12.2(33)SRA	In 12.2(33)SRA, support was added for the Cisco 7600 series routers.
	12.4(11)T	In 12.4(11)T, this feature was integrated into the release.
	12.2(33)SXH	In 12.2(33)SXH, this feature was integrated into the release.

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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# NSF/SSO—Any Transport over MPLS and AToM Graceful Restart

---

**First Published: August 11, 2004**

**Last Updated: February 27, 2009**

The NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature allows Any Transport over MPLS (AToM) to use Cisco nonstop forwarding (NSF), stateful switchover (SSO), and Graceful Restart (GR) to allow a Route Processor (RP) to recover from a disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

NSF with SSO is effective at increasing availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.



## Note

In this document, the NSF/SSO—Any Transport over MPLS and AToM Graceful Restart feature is referred to as AToM NSF for brevity.

---

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for AToM NSF” section on page 10](#).

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



---

**Americas Headquarters:**

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



# Contents

- [Prerequisites for AToM NSF, page 2](#)
- [Restrictions for AToM NSF, page 3](#)
- [Information About AToM NSF, page 4](#)
- [Configuration Examples for AToM NSF, page 6](#)
- [Additional References, page 8](#)
- [Command Reference, page 9](#)
- [Feature Information for AToM NSF](#)

## Prerequisites for AToM NSF

Before you can configure AToM NSF, make sure the following tasks have been completed:

- AToM virtual circuits (VCs) have been configured on the router. See the [Any Transport over MPLS](#) feature module for information on configuring AToM. For configuring L2VPN Interworking, see the [L2VPN Interworking](#) feature module.
- SSO has been configured on the Route Processors. See the [Stateful Switchover](#) feature module for configuration information.
- Nonstop forwarding has been configured on the routers. You must enable nonstop forwarding on the routing protocols running between the P routers, PE routers, and CE routers. The routing protocols are Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS), and Border Gateway Protocol (BGP). See the [Cisco Nonstop Forwarding](#) feature module for configuration information.

This section lists the following prerequisites:

- [Supported Hardware, page 2](#)
- [Neighbor Routers in the MPLS HA Environment, page 3](#)
- [Stateful Switchover, page 3](#)
- [Nonstop Forwarding for Routing Protocols, page 3](#)

## Supported Hardware

For hardware requirements for this feature, see the following documents:

- For Cisco IOS Release 12.2(25)S, see the “Supported Hardware” section of the *Cross-Platform Release Notes for Cisco IOS Release 12.2S*.

The URL is:

[http://www.cisco.com/en/US/docs/ios/12\\_2s/release/notes/122Srn.html](http://www.cisco.com/en/US/docs/ios/12_2s/release/notes/122Srn.html)

- For Cisco IOS Release 12.2(28)SB, see the “Supported Hardware” section of the *Cross-Platform Release Notes for Cisco IOS Release 12.2SB*.

The URL is:

[http://www.cisco.com/en/US/docs/ios/12\\_2sb/release/notes/122SB.html](http://www.cisco.com/en/US/docs/ios/12_2sb/release/notes/122SB.html)

- For Cisco IOS Release 12.2(33)SRC, see the “Supported Hardware” section of the *Release Notes for Cisco IOS Release 12.2SR for the Cisco 7600 Series Routers*.

The URL is:

[http://www.cisco.com/en/US/docs/ios/12\\_2sr/release/notes/122SRrn.html](http://www.cisco.com/en/US/docs/ios/12_2sr/release/notes/122SRrn.html)

## Neighbor Routers in the MPLS HA Environment

AToM NSF requires that neighbor networking devices be able to perform AToM GR. In Cisco IOS Releases 12.2(25)S and 12.2(28)SB, the Cisco 7200 and Cisco 7500 routers are capable of supporting AToM GR and can be used as neighbor networking devices.

In Cisco IOS Release 12.2(33)SRC, the Cisco 7600 routers are capable of supporting AToM high availability (HA) and MPLS Label Distribution Protocol (LDP) GR.

## Stateful Switchover

To perform AToM NSF, Route Processors must be configured for SSO and GR. See the *Stateful Switchover* feature module for more information.

## Nonstop Forwarding for Routing Protocols

You must enable NSF on the routing protocols running between the provider (P) routers, provider edge (PE) routers, and customer edge (CE) routers. The routing protocols are the following:

- Border Gateway Protocol (BGP)
- Open Shortest Path First (OSPF)
- Intermediate System-to-Intermediate System (IS-IS)

See the *Cisco Nonstop Forwarding* feature module for more information.

## Restrictions for AToM NSF

AToM NSF includes the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- AToM NSF cannot be configured on label-controlled ATM (LC-ATM) interfaces.
- AToM NSF supports AToM Layer 2 Virtual Private Network (L2VPN) Interworking. However, Layer 2 Tunnel Protocol Version 3 (L2TPv3) Interworking is not supported.
- AToM NSF interoperates with Layer 2 local switching. However, AToM NSF has no effect on interfaces configured for local switching.
- To allow distributed Cisco Express Forwarding to work on the interfaces, disable fair queueing on serial interfaces.
- On the Cisco 7500 series routers, distributed Cisco Express Forwarding is needed to support AToM NSF.
- The Cisco 7500 router does not support AToM Ethernet-VLAN interworking IP; however, AToM Ethernet-VLAN interworking Ethernet is supported.

# Information About AToM NSF

To configure AToM NSF, you should understand the following concepts:

- [How AToM NSF Works, page 4](#)
- [AToM Information Checkpointing, page 4](#)
- [ISSU Support, page 5](#)

## How AToM NSF Works

AToM NSF improves the availability of a service provider's network that uses AToM to provide Layer 2 VPN services to its customers. HA provides the ability to detect failures and handle them with minimal disruption to the service being provided. AToM NSF is achieved by SSO and NSF mechanisms. A standby RP provides control-plane redundancy. The control plane state and data plane provisioning information for the attachment circuits (ACs) and AToM pseudowires (PWs) are checkpointed to the standby RP to provide NSF for AToM L2VPNs.

## AToM Information Checkpointing

Checkpointing is a function that copies state information from the active RP to the backup RP, thereby ensuring that the backup RP has the latest information. If the active RP fails, the backup RP can take over.

For the AToM NSF feature, the checkpointing function copies the active RP's information bindings to the backup RP. The active RP sends updates to the backup RP when information is modified.

To display checkpointing data, issue the **show acircuit checkpoint** command on the active and backup RPs. The active and backup RPs have identical copies of the information.

## Checkpointing Troubleshooting Tips

To help troubleshoot checkpointing errors, use the following commands:

- Use the **debug acircuit checkpoint** command to enable checkpointing debug messages for ACs.
- Use the **debug mpls l2transport checkpoint** command to enable checkpointing debug messages for AToM.
- Use the **show acircuit checkpoint** command to display the AC checkpoint information.
- Use the **show mpls l2transport checkpoint** command to display whether checkpointing is allowed, how many AToM VCs were bulk-synchronized (on the active RP), and how many AToM VCs have checkpoint data (on the standby RP).
- Use the **show mpls l2transport vc detail** command to display details of VC checkpointed information.

## ISSU Support

Beginning with Cisco IOS Release 12.2(33)SRC, AToM NSF supports In Service Software Upgrade (ISSU) capability. Virtual Private LAN Services (VPLS) NSF/SSO and HA with ISSU work together to enable upgrades or downgrades of a Cisco IOS image without control and data plane outages. With ISSU, all message data structures that are used for checkpointing and exchanges between the active RP and standby RP are versioned.

## Configuring MPLS LDP Graceful Restart

Before you configure AToM NSF, you need to configure MPLS LDP Graceful Restart.


MPLS LDP GR is enabled globally. When you enable LDP GR, it has no effect on existing LDP sessions. LDP GR is enabled for new sessions that are established after the feature has been globally enabled.

Perform this task to configure MPLS LDP GR.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef [distributed]**
4. **mpls ldp graceful-restart**
5. **interface type slot/port**
6. **mpls ip**
7. **mpls label protocol {ldp | tdp | both}**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef [distributed]</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables Cisco Express Forwarding.   <b>Note</b> In Cisco ASR 1000 series Aggregation Services Routers, the <b>distributed</b> keyword is mandatory.
Step 4	<b>mpls ldp graceful-restart</b>  <b>Example:</b> Router (config)# mpls ldp graceful-restart	Enables the router to protect the LDP bindings and MPLS forwarding state during a disruption in service.

	Command or Action	Purpose
Step 5	<pre>interface type slot/port</pre> <p><b>Example:</b> Router(config)# interface pos 3/0</p>	Specifies an interface and enters interface configuration mode.
Step 6	<pre>mpls ip</pre> <p><b>Example:</b> Router(config-if)# mpls ip</p>	Configures MPLS hop-by-hop forwarding for an interface.
Step 7	<pre>mpls label protocol {ldp   tdp   both}</pre> <p><b>Example:</b> Router(config-if)# mpls label protocol ldp</p>	Configures the use of LDP for an interface. <ul style="list-style-type: none"> <li>You must use LDP, because TDP sessions are not supported.</li> <li>You can also issue the <b>mpls label protocol ldp</b> command in global configuration mode, which enables LDP on all interfaces configured for MPLS.</li> </ul>

## Configuration Examples for AToM NSF

This section provides the following configuration example:

- [Ethernet to VLAN Interworking with AToM NSF: Example, page 7](#)

## Ethernet to VLAN Interworking with AToM NSF: Example

The following example shows how to configure AToM NSF on two PE routers:

PE1	PE2
<pre> ip cef distributed ! redundancy mode sso ! boot system flash disk2:rsp-pv-mz ! mpls ldp graceful-restart mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 force mpls ldp advertise-labels ! pseudowire-class atom-eth   encapsulation mpls   interworking ethernet ! interface Loopback0   ip address 10.8.8.8 255.255.255.255 ! interface FastEthernet1/1/0   xconnect 10.9.9.9 123 encap mpls pw-class atom-eth  interface POS6/1/0   ip address 10.1.1.1 255.255.255.0   mpls ip   mpls label protocol ldp   clock source internal   crc 32 ! interface Loopback0   ip address 10.8.8.8 255.255.255.255   no shutdown ! router ospf 10   nsf   network 10.8.8.8 0.0.0.0 area 0   network 19.1.1.1 0.0.0.0 area 0 </pre>	<pre> ip cef distributed ! redundancy mode sso ! boot system flash disk2:rsp-pv-mz ! mpls ldp graceful-restart mpls ip mpls label protocol ldp mpls ldp router-id Loopback0 force mpls ldp advertise-labels ! pseudowire-class atom-eth   encapsulation mpls   interworking eth ! interface Loopback0   ip address 10.9.9.9 255.255.255.255 ! interface FastEthernet3/0/0   ip route-cache cef ! interface FastEthernet3/0/0.3   encapsulation dot1Q 10   xconnect 10.8.8.8 123 encap mpls pw-class atom-eth  interface POS1/0/0   ip address 10.1.1.2 255.255.255.0   mpls ip   mpls label protocol ldp   clock source internal   crc 32 ! interface Loopback0   ip address 10.9.9.9 255.255.255.255 ! router ospf 10   nsf   network 10.9.9.9 0.0.0.0 area 0   network 10.1.1.2 0.0.0.0 area 0 </pre>

# Additional References

The following sections provide references related to AToM NSF.

## Related Documents

Related Topic	Document Title
Stateful switchover	<a href="#"><i>Stateful Switchover</i></a>
MPLS Label Distribution Protocol	<a href="#"><i>MPLS Label Distribution Protocol (LDP)</i></a>
Cisco nonstop forwarding	<a href="#"><i>Cisco Nonstop Forwarding</i></a>
Any Transport over MPLS	<a href="#"><i>Any Transport over MPLS</i></a>
L2VPN Interworking configuration	<a href="#"><i>L2VPN Interworking</i></a>

## Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIBs	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
RFC 3036	<i>LDP Specification</i>
RFC 3478	<i>Graceful Restart Mechanism for Label Distribution</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug acircuit checkpoint**
- **debug mpls l2transport checkpoint**
- **show acircuit checkpoint**
- **show mpls l2transport checkpoint**
- **show mpls l2transport vc**



# Feature Information for AToM NSF

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for AToM NSF Any Transport over MPLS and AToM Graceful Restart

Feature Name	Releases	Feature Information
AToM NSF	12.2(25)S 12.2(28)SB 12.2(33)SRC	This feature uses NSF, SSO, and Graceful Restart to allow a Route Processor to recover from a disruption in control plane service without losing its MPLS forwarding state.  In 12.2(25)S, this feature was introduced on the Cisco 7500 series router.  In 12.2(28)SB, this feature was integrated into the release.  In 12.2(33)SRC, this feature was integrated into the release for the Cisco 7600 router. Support for ISSU was added.

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

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

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

©2004–2009 Cisco Systems, Inc. All rights reserved.



# NSF/SSO—MPLS TE and RSVP Graceful Restart

---

**First Published: August 2, 2004**

**Last Updated: October 21, 2009**

The NSF/SSO—MPLS TE and RSVP Graceful Restart feature allows a Route Processor (RP) to recover from disruption in control plane service without losing its Multiprotocol Label Switching (MPLS) forwarding state.

Cisco nonstop forwarding (NSF) with stateful switchover (SSO) provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

In Cisco IOS Release 12.2(33)SRE, SSO can co-exist with traffic engineering (TE) primary tunnels, backup tunnels, and automesh tunnels.

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the “[Feature Information for NSF/SSO—MPLS TE and RSVP Graceful Restart](#)” section on [page 14](#).

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

## Content

- [Prerequisites for NSF/SSO—MPLS TE and RSVP Graceful Restart, page 2](#)
- [Restrictions for NSF/SSO—MPLS TE and RSVP Graceful Restart, page 2](#)
- [Information About NSF/SSO—MPLS TE and RSVP Graceful Restart, page 3](#)
- [How to Configure NSF/SSO—MPLS TE and RSVP Graceful Restart, page 5](#)



---

**Americas Headquarters:**

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

© 2009 Cisco Systems, Inc. All rights reserved.

- [Configuration Examples for NSF/SSO—MPLS TE and RSVP Graceful Restart, page 11](#)
- [Additional References, page 12](#)
- [Feature Information for NSF/SSO—MPLS TE and RSVP Graceful Restart, page 14](#)
- [Glossary, page 15](#)

## Prerequisites for NSF/SSO—MPLS TE and RSVP Graceful Restart

- Configure Resource Reservation Protocol (RSVP) graceful restart in full mode.
  - Configure RSVP graceful restart on all interfaces of the neighbor that you want to be restart-capable.
  - Configure the redundancy mode as SSO. See [Stateful Switchover](#).
  - Enable NSF on the routing protocols running among the provider routers (P), provider edge (PE) routers, and customer edge (CE) routers. The routing protocols are as follows:
    - Border Gateway Protocol (BGP)
    - Open Shortest Path First (OSPF)
    - Intermediate System-to-Intermediate System (IS-IS)
- For more information, see [Information about Cisco Nonstop Forwarding](#).
- Enable MPLS.
  - Configure traffic engineering (TE).

## Restrictions for NSF/SSO—MPLS TE and RSVP Graceful Restart

- RSVP graceful restart supports node failure only.
- Unnumbered interfaces are not supported.
- You cannot enable RSVP fast reroute (FRR) hello messages and RSVP graceful restart on the same router.
- Configure this feature on Cisco 7600 series routers with dual RPs only.
- For releases prior to Cisco IOS Release 12.2(33)SRE, you cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with SSO and Route Processor Redundancy Plus (RPR+). This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered if any midpoint router along the label-switched path (LSP) of the router experiences an SSO. For Cisco IOS Release 12.2(33)SRE, go to the [“MPLS TE Autotunnel and SSO Coexistence” section on page 5](#).
- MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.
- When you configure RSVP graceful restart, you must use the neighbor’s interface IP address.

# Information About NSF/SSO—MPLS TE and RSVP Graceful Restart

To configure the NSF/SSO—MPLS TE and RSVP Graceful Restart feature, you should understand the following concepts:

- [Overview of MPLS TE and RSVP Graceful Restart, page 3](#)
- [MPLS TE Autotunnel and SSO Coexistence, page 5](#)
- [Benefits of MPLS TE and RSVP Graceful Restart, page 5](#)

## Overview of MPLS TE and RSVP Graceful Restart

RSVP graceful restart allows RSVP TE-enabled nodes to recover gracefully following a node failure in the network such that the RSVP state after the failure is restored as quickly as possible. The node failure may be completely transparent to other nodes in the network.

RSVP graceful restart preserves the label values and forwarding information and works with third-party or Cisco routers seamlessly.

RSVP graceful restart depends on RSVP hello messages to detect that a neighbor went down. Hello messages include Hello Request or Hello Acknowledgment (ACK) objects between two neighbors.

A node hello is transmitted when Graceful Restart is globally configured and the first LSP to the neighbor is created.

Interface Hello is an optional configuration. If the Graceful Restart Hello command is configured on an interface, the interface hello is considered to be an additional hello instance with the neighbor.

An interface hello for Graceful Restart is transmitted when all of the following conditions are met:

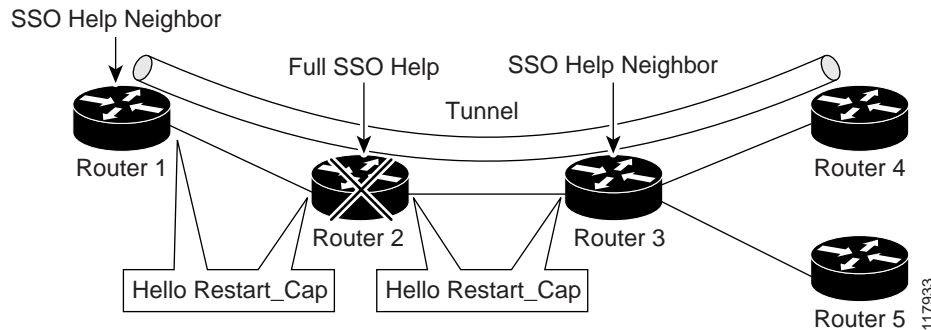
- Graceful Restart is configured globally.
- Graceful restart is configured on the interface.
- An LSP to the neighbor is created and goes over the interface.

Cisco recommends that you use node hellos if the neighbor supports node hellos, and configure interface hellos only if the neighbor router does not support node hellos.

Interface hellos differ from node hellos, as follows:

- **Interface hello**—The source address in the IP header of the hello message has an IP address that matches the interface that the Hello message sent out. The destination address in the IP header is the interface address of the neighbor on the other side of the link. A TTL of 1 is used for per-interface hellos as it is destined for the directly-connected neighbor.
- **Node hello**—The source address in the IP header of the Hello message includes the TE router ID of the sending router. The destination address of the IP header has the router ID of the neighbor to which this message is sent. A TTL of more than 1 is used.

As shown in [Figure 1](#), the RSVP graceful restart extension to these messages adds an object called Hello Restart\_Cap, which tells neighbors that a node may be capable of recovering if a failure occurs.

**Figure 1** *How RSVP Graceful Restart Works*

The Hello Restart\_Cap object has two values: the restart time, which is the sender's time to restart the RSVP\_TE component and exchange hello messages after a failure; and the recovery time, which is the desired time that the sender wants the receiver to synchronize the RSVP and MPLS databases.

In Figure 1, RSVP graceful restart help neighbor support is enabled on Routers 1 and 3 so that they can help a neighbor recover after a failure, but they cannot perform self recovery. Router 2 has full SSO help support enabled, meaning it can perform self recovery after a failure or help its neighbor to recover. Router 2 has two RPs, one that is active and one that is standby (backup). A TE LSP is signaled from Router 1 to Router 4.

Router 2 performs checkpointing; that is, it copies state information from the active RP to the standby RP, thereby ensuring that the standby RP has the latest information. If an active RP fails, the standby RP can take over.

Routers 2 and 3 exchange periodic graceful restart hello messages every 10,000 milliseconds (ms) (10 seconds), and so do Routers 2 and 1 and Routers 3 and 4. Assume that Router 2 advertises its restart time = 60,000 ms (60 seconds) and its recovery time = 60,000 ms (60 seconds) as shown in the following example:

```
23:33:36: Outgoing Hello:
23:33:36:  version:1 flags:0000 cksum:883C ttl:255 reserved:0 length:32
23:33:36:  HELLO                               type HELLO REQUEST length 12:
23:33:36:    Src_Instance: 0x6EDA8BD7, Dst_Instance: 0x00000000
23:33:36:  RESTART_CAP                               type 1 length 12:
23:33:36:    Restart_Time: 0x0000EA60, Recovery_Time: 0x0000EA60
```

Router 3 records this into its database. Also, both neighbors maintain the neighbor status as UP. However, Router 3's control plane fails at some point (for example, a primary RP failure). As a result, RSVP and TE lose their signaling information and states although data packets continue to be forwarded by the line cards.

When Router 3 declares communication with Router 2 lost, Router 3 starts the restart time to wait for the duration advertised in Router 2's restart time previously recorded (60 seconds). Routers 1 and 2 suppress all RSVP messages to Router 3 except hellos. Router 3 keeps sending the RSVP PATH and RESV refresh messages to Routers 4 and 5 so that they do not expire the state for the LSP; however, Routers 1 and 3 suppress these messages for Router 2.

When Routers 1 and 3 receive the hello message from Router 2, Routers 1 and 3 check the recovery time value in the message. If the recovery time is 0, Router 3 knows that Router 2 was not able to preserve its forwarding information, and Routers 1 and 3 delete all RSVP state that they had with Router 2.

If the recovery time is greater than 0, Router 1 sends Router 2 PATH messages for each LSP that it had previously sent through Router 2. If these messages were previously refreshed in summary messages, they are sent individually during the recovery time. Each of these PATH messages includes a Recovery\_Label object containing the label value received from Router 2 before the failure.

When Router 3 receives a PATH message from Router 2, Router 3 sends a RESV message upstream. However, Router 3 suppresses the RESV message until it receives a PATH message. When Router 2 receives the RESV message, it installs the RSVP state and reprograms the forwarding entry for the LSP.

## MPLS TE Autotunnel and SSO Coexistence

In Cisco IOS 12.2(33)SRE and later releases, MPLS TE primary tunnels, backup tunnels, and automesh tunnels can coexist with SSO; that is, they can be configured together. However, there are the following functional differences:

- Headend autotunnels created on the active RP are not checkpointed and created on the standby RP.
- After the SSO switchover, the new active RP recreates all the headend autotunnels and signals their LSPs. The LSP ID is different from the LSP ID used before the SSO switchover. Tunnel traffic may be dropped during the signaling of new autotunnel LSPs.
- SSO coexistence does not affect TE autotunnels in the midpoint or tailend routers along the LSPs from being checkpointed and recovered.

## Benefits of MPLS TE and RSVP Graceful Restart

### State Information Recovery

RSVP graceful restart allows a node to perform self recovery or to help its neighbor recover state information when there is an RP failure or the device has undergone an SSO.

### Session Information Recovery

RSVP graceful restart allows session information recovery with minimal disruption to the network.

### Increased Availability of Network Services

A node can perform a graceful restart to help itself or a neighbor recover its state by keeping the label bindings and state information, thereby providing a faster recovery of the failed node and not affecting currently forwarded traffic.

## How to Configure NSF/SSO—MPLS TE and RSVP Graceful Restart

This section contains the following procedures:

- [Enabling RSVP Graceful Restart Globally, page 6](#) (required)
- [Enabling RSVP Graceful Restart on an Interface, page 6](#) (required)
- [Setting a DSCP Value, page 7](#) (optional)
- [Setting a Value to Control the Hello Refresh Interval, page 8](#) (optional)
- [Setting a Value to Control the Missed Refresh Limit, page 9](#) (optional)
- [Verifying the RSVP Graceful Restart Configuration, page 10](#) (optional)

## Enabling RSVP Graceful Restart Globally

Perform this task to enable RSVP graceful restart globally.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart mode {help-neighbor | full}**
4. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip rsvp signalling hello graceful-restart mode {help-neighbor   full}</b>  <b>Example:</b> Router(config)# ip rsvp signalling hello graceful-restart mode full	Enables RSVP TE graceful restart capability on an RP. <ul style="list-style-type: none"><li>• Enter the <b>help-neighbor</b> keyword to enable a neighboring router to restart after a failure.</li><li>• Enter the <b>full</b> keyword to enable a router to perform self recovery or to help a neighbor recover after a failure.</li></ul>
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	(Optional) Returns to privileged EXEC mode.

## Enabling RSVP Graceful Restart on an Interface

Perform this task to enable RSVP graceful restart on an interface.



#### Note

You must repeat this procedure for each of the neighbor router's interfaces.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*

4. Repeat Step 3 as needed to configure additional interfaces.
5. **ip rsvp signalling hello graceful-restart neighbor *ip-address***
6. Repeat Step 5 as needed to configure additional IP addresses on a neighbor router's interfaces.
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface <i>type number</i></b>  <b>Example:</b> Router(config)# interface POS 1/0/0	Configures the interface type and number and enters interface configuration mode.
Step 4	Repeat Step 3 as needed to configure additional interfaces.	(Optional) Configures additional interfaces.
Step 5	<b>ip rsvp signalling hello graceful-restart neighbor <i>ip-address</i></b>  <b>Example:</b> Router(config-if)# ip rsvp signalling hello graceful-restart neighbor 10.0.0.0	Enables support for RSVP graceful restart on routers helping their neighbors recover TE tunnels following SSO. <p><b>Note</b> The IP address must be that of the neighbor's interface.</p>
Step 6	Repeat Step 5 as needed to configure additional IP addresses on a neighbor router's interfaces.	(Optional) Configures additional IP addresses on a neighbor router's interfaces.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit	(Optional) Returns to privileged EXEC mode.

## Setting a DSCP Value

Perform this task to set a differentiated services code point (DSCP) value.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart dscp *num***



4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip rsvp signalling hello graceful-restart dscp num</b>  <b>Example:</b> Router(config)# ip rsvp signalling hello graceful-restart dscp 30	Sets a DSCP value on a router with RSVP graceful restart enabled.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	(Optional) Returns to privileged EXEC mode.

## Setting a Value to Control the Hello Refresh Interval

Perform this task to set a value to control the hello refresh interval.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart refresh interval *interval-value***
4. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip rsvp signalling hello graceful-restart refresh interval interval-value</b>  <b>Example:</b> Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000	Sets the value to control the request interval in graceful restart hello messages. This interval represents the frequency at which RSVP hello messages are sent to a neighbor; for example, one hello message is sent per each interval.  <b>Note</b> If you change the default value for this command and you also changed the RSVP refresh interval using the <b>ip rsvp signalling refresh interval</b> command, ensure that the value for the <b>ip rsvp signalling hello graceful-restart refresh interval</b> command is less than the value for the <b>ip rsvp signalling hello refresh interval</b> command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after an SSO has occurred.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	(Optional) Returns to privileged EXEC mode.

## Setting a Value to Control the Missed Refresh Limit

Perform this task to set a value to control the missed refresh limit.

## SUMMARY STEPS

1. enable
2. configure terminal
3. ip rsvp signalling hello graceful-restart refresh misses *msg-count*
4. exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip rsvp signalling hello graceful-restart refresh misses msg-count</b>  <b>Example:</b> Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5	Specifies how many sequential RSVP TE graceful restart hello acknowledgments (ACKs) a node can miss before the node considers communication with its neighbor lost.  <b>Note</b> If you change the default value for this command and you are also using the <b>ip rsvp signalling hello refresh misses</b> command, ensure that the value for the <b>ip rsvp signalling hello graceful-restart refresh misses</b> command is less than the value for the <b>ip rsvp signalling hello refresh misses</b> command. Otherwise, some or all of the LSPs may not be recovered after an SSO has occurred.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	(Optional) Returns to privileged EXEC mode.

## Verifying the RSVP Graceful Restart Configuration

Perform this task to verify the RSVP graceful restart configuration.

## SUMMARY STEPS

1. enable
2. show ip rsvp hello graceful-restart
3. exit

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	(Optional) Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>show ip rsvp hello graceful-restart</b>  <b>Example:</b> Router# show ip rsvp hello graceful-restart	Displays information about the status of RSVP graceful restart and related parameters.
Step 3	<b>exit</b>  <b>Example:</b> Router# exit	(Optional) Returns to user EXEC mode.

## Configuration Examples for NSF/SSO—MPLS TE and RSVP Graceful Restart

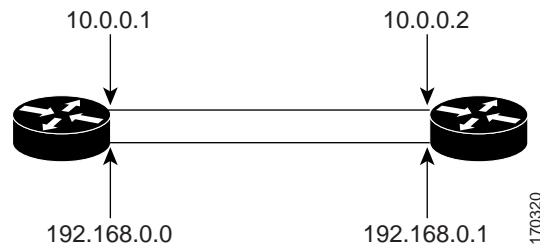
This section provides the following configuration examples:

- [Configuring NSF/SSO—MPLS TE and RSVP Graceful Restart: Example, page 11](#)
- [Verifying the NSF/SSO—MPLS TE and RSVP Graceful Restart Configuration: Example, page 12](#)

### Configuring NSF/SSO—MPLS TE and RSVP Graceful Restart: Example

In the following example, RSVP graceful restart is enabled globally and on a neighbor router's interfaces as shown in [Figure 2](#). Related parameters, including a DSCP value, a refresh interval, and a missed refresh limit are set.

**Figure 2**      **Sample Network Configuration**



```

enable
configure terminal
ip rsvp signalling hello graceful-restart mode full
interface POS 1/0/0
 ip rsvp signalling hello graceful-restart neighbor 10.0.0.1
 ip rsvp signalling hello graceful-restart neighbor 10.0.0.2
exit

```

```
ip rsvp signalling hello graceful-restart dscp 30
ip rsvp signalling hello graceful-restart refresh interval 50000
ip rsvp signalling hello graceful-restart refresh misses 5
exit
```

## Verifying the NSF/SSO—MPLS TE and RSVP Graceful Restart Configuration: Example

The following example verifies the status of RSVP graceful restart and the configured parameters:

```
Router# show ip rsvp hello graceful-restart
```

```
Graceful Restart: Enabled (full mode)
Refresh interval: 10000 msecs
Refresh misses: 4
DSCP:0x30
Advertised restart time: 30000 msecs
Advertised recovery time: 120000 msecs
Maximum wait for recovery: 3600000 msecs
```

## Additional References

The following sections provide references related to the NSF/SSO—MPLS TE and RSVP Graceful Restart feature.

## Related Documents

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<a href="#">Cisco IOS Quality of Service Solutions Command Reference</a>
Quality of service (QoS) classification	<a href="#">Classification Overview</a>
QoS signalling	<a href="#">Signalling Overview</a>
QoS congestion management	<a href="#">Congestion Management Overview</a>
Stateful switchover	<a href="#">Stateful Switchover</a>
Cisco nonstop forwarding	<a href="#">Information about Cisco Nonstop Forwarding</a>
RSVP hello state timer	<a href="#">MPLS Traffic Engineering: RSVP Hello State Timer</a>

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3209	RSVP-TE: Extensions to RSVP for LSP Tunnels
RFC 3473	<i>Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions</i>
RFC 4558	Node-ID Based Resource Reservation Protocol (RSVP) Hello: A Clarification Statement

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for NSF/SSO—MPLS TE and RSVP Graceful Restart

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

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



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

**Table 1** Feature Information for NSF/SSO—MPLS TE and RSVP Graceful Restart

Feature Name	Releases	Feature Information
NSF/SSO—MPLS TE and RSVP Graceful Restart	12.0(29)S 12.2(33)SRA 12.2(33)SRB 12.2(33)SXH 12.2(33)SRE	<p>The NSF/SSO—MPLS TE and RSVP Graceful Restart feature allows an RP or its neighbor to recover from disruption in control plane service without losing its MPLS forwarding state.</p> <p>In Cisco IOS Release 12.0(29)S, this feature was introduced as MPLS Traffic Engineering—RSVP Graceful Restart and allowed a neighboring RP to recover from disruption in control plane service without losing its MPLS forwarding state.</p> <p>In Cisco IOS Release 12.2(33)SRA, this feature was integrated and new commands were added.</p> <p>In Cisco IOS Release 12.2(33)SRB, support was added for ISSU and SSO recovery of LSPs that include loose hops.</p> <p>In Cisco IOS Release 12.2(33)SXH, this feature was integrated.</p> <p>In Cisco IOS Release 12.2(33)SRE, SSO can coexist with primary tunnels, backup tunnels, and mesh tunnels.</p>

# Glossary

**DSCP**—differentiated services code point. Six bits in the IP header, as defined by the IETF. These bits determine the class of service provided to the IP packet.

**Fast Reroute**—A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**graceful restart**—A process for helping an RP restart after a node failure has occurred.

**headend**—The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hello instance**—A mechanism that implements the RSVP hello extensions for a given router interface address and remote IP address. Active hello instances periodically send hello request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**IGP**—Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

**ISSU**—In Service Software Upgrade. Software upgrade without service interruption.

**label**—A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

**LSP**—label switched path. A configured connection between two routers, in which MPLS is used to carry packets.

**MPLS**—Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. MPLS enables routers at the edge of a network to apply labels to packets (frames). ATM switches or existing routers in the network core can switch packets according to the labels.

**RSVP**—Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

**state**—Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**tailend**—The router upon which an LSP is terminated. This is the last router in the LSP's path.

**TE**—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.



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

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

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

© 2004–2009 Cisco Systems, Inc. All rights reserved.



# NSF/SSO/ISSU Support for VPLS

---

**First Published: January 7, 2008**

**Last Updated: January 7, 2008**

Virtual Private LAN Services (VPLS), with nonstop forwarding (NSF), stateful switchover (SSO), and in service software upgrade (ISSU) support, improves the availability of service provider networks that use VPLS for multipoint Layer 2 virtual private network (VPN) services. Cisco NSF with SSO is effective at increasing availability of network services. Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service in the event of a critical failure in the primary processor, while SSO synchronizes the network state information between the primary and the secondary processor.

In conjunction with VPLS NSF/SSO, VPLS High Availability (HA) features include the ISSU capability. Working together, ISSU and NSF/SSO enable upgrades or downgrades of a Cisco IOS image without control and data plane outages.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your Cisco IOS software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [Feature Information for NSF/SSO/ISSU Support for VPLS, page 26](#).

## Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

## Contents

- [Prerequisites for NSF/SSO/ISSU Support for VPLS, page 2](#)
- [Restrictions for NSF/SSO/ISSU Support for VPLS, page 2](#)
- [Information About NSF/SSO/ISSU Support for VPLS, page 2](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [How to Configure NSF/SSO/ISSU Support for VPLS, page 3](#)
- [Verifying and Troubleshooting NSF/SSO/ISSU Support for VPLS, page 4](#)
- [Configuration Examples for NSF/SSO/ISSU Support for VPLS, page 10](#)
- [Additional References, page 24](#)
- [Command Reference, page 25](#)
- [Feature Information for NSF/SSO/ISSU Support for VPLS, page 26](#)

## Prerequisites for NSF/SSO/ISSU Support for VPLS

This section lists the following prerequisites that are required to use the NSF/SSO/ISSU Support for VPLS feature.

You must configure the following features on your network:

- VPLS (see the “Virtual Private LAN Services on the Optical Services Modules” chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*, Release 12.2SR)
- VPLS Autodiscovery (see *VPLS Autodiscovery: BGP Based* and *BGP Support for the L2VPN Address Family*)
- NSF/SSO: Any Transport over MPLS (see *NSF/SSO—Any Transport over MPLS and AToM Graceful Restart*)
- NSF/SSO router support on the 7600 router (see the “Configuring NSF with SSO Supervisor Engine Redundancy” chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*, Release 12.2SR)
- ISSU router support on the 7600 router (see the “ISSU and eFSU on Cisco 7600 Series Routers” chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*, Release 12.2SR)

## Restrictions for NSF/SSO/ISSU Support for VPLS

The NSF/SSO/ISSU Support for VPLS feature has the following restrictions:

- NSF/SSO/ISSU support for VPLS does not include support for PWs to auto discovered neighbors via Border Gateway Protocol (BGP). Statically configured neighbors are supported.
- For supported hardware, see the Cisco Release 12.2SR Release Notes.
- NSF/SSO/ISSU support for VPLS does not include support for line cards that do not support Minimal Disruptive Restart (MDR) or pre downloading of firmware or driver code.

## Information About NSF/SSO/ISSU Support for VPLS

To configure the NSF/SSO/ISSU Support for VPLS feature, you should understand the following concepts:

- [How NSF/SSO Works with VPLS, page 3](#)
- [How ISSU Works with VPLS, page 3](#)

## How NSF/SSO Works with VPLS

VPLS with NSF/SSO support improves the availability of service provider networks that use VPLS for multipoint Layer 2 VPN services. HA minimizes service disruptions that can occur if a system failure occurs. To address failures, VPLS HA includes SSO and NSF mechanisms using a standby Route Processor (RP) to provide control-plane redundancy. VPLS NSF is achieved by SSO and NSF mechanisms.

While the standby RP transitions to the active RP, packet forwarding either continues forwarding on line card(s) or packet forwarding is switched over (switchover) to other hardware devices associated with the newly active RP.

## How ISSU Works with VPLS

In conjunction with VPLS NSF/SSO, VPLS HA includes ISSU, a comprehensive in-service upgrade solution for the IP/MPLS edge. ISSU minimizes network downtime due to software upgrades and maintenance activities. ISSU allows upgrades or downgrades to Cisco IOS software images with no effect on the control plane and minimal effect on system packet forwarding. With ISSU, all message data structures used for checkpointing, and exchanges between the active RP and standby RP are versioned.

To perform an in-service upgrade, the standby RP in a dual RP-based platform (such as the Cisco 7600 router) is first loaded with the desired Cisco IOS software release. The standby RP then comes up as a hot-standby RP with an upgraded version of the software, and a switchover is performed to transfer control to the standby RP and run the upgraded image.

During the ISSU procedure, supported SSO protocols and features maintain their session states with no disruption of the Layer 2 protocol sessions. Cisco NSF technology is used to continue packet forwarding during the software upgrade procedure while the routing information is re-created on the newly active RP. The result is a seamless software upgrade for an IP/MPLS provider edge router with no disruptions to Layer 2 protocol sessions and minimal effect on packet forwarding.

### Benefits

Primary benefits for ISSU are:

- Rapid, nondisruptive feature deployment—By preserving user sessions and minimizing packet loss during software upgrades, ISSU helps enable rapid, nondisruptive deployments for new features and services at the IP/MPLS provider edge.
- Comprehensive solution for planned downtime—ISSU addresses the entire spectrum of software upgrade needs, from applying caveat fixes to deploying new features and services, and delivers a comprehensive solution for addressing planned network downtime.
- Increased operational efficiencies—ISSU minimizes and streamlines planned downtime and helps enable operational process changes for software deployment, significantly decreasing planned downtime effort and expenses and increasing operational efficiency.

## How to Configure NSF/SSO/ISSU Support for VPLS

This section contains the following procedures:

- [Configuring VPLS, page 4](#) (required)
- [Configuring NSF/SSO: Any Transport over MPLS, page 4](#) (required)

- [Configuring NSF/SSO Router support, page 4](#) (required)
- [Configuring ISSU Router Support, page 4](#) (required)

## Configuring VPLS

VPLS must be configured on the router. See the “Virtual Private LAN Services on the Optical Services Modules” chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*, Release 12.2SR for information on configuring VPLS.

## Configuring NSF/SSO: Any Transport over MPLS

You must configure the NSF/SSO: Any Transport over MPLS feature on the router. See the *NSF/SSO—Any Transport over MPLS and AToM Graceful Restart* feature module for information on configuring the NSF/SSO: Any Transport over MPLS feature.

## Configuring NSF/SSO Router support

You must configure NSF/SSO router support on the Cisco 7600 router. See the “Configuring NSF with SSO Supervisor Engine Redundancy” chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*, Release 12.2SR for information on configuring the NSF with SSO Supervisor Engine Redundancy feature.

## Configuring ISSU Router Support

You must configure ISSU router support on the Cisco 7600 router.

- See the “ISSU and eFSU on Cisco 7600 Series Routers” chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*, Release 12.2SR for information on configuring ISSU and Enhanced Fast Software Upgrade (eFSU) on Cisco 7600 series routers.

## Verifying and Troubleshooting NSF/SSO/ISSU Support for VPLS

To verify the NSF/SSO/ISSU Support for VPLS configuration, use the following show and debug commands:

### DETAILED STEPS

1. **show checkpoint clients**
2. **show vfi [name vfi-name] checkpoint [summary]**
3. **debug cwan atom**
4. **debug cwan ltl**
5. **debug issu client negotiation**
6. **debug issu client registration**

**7. debug issu client transform****8. debug vfi checkpoint****DETAILED STEPS****Step 1 show checkpoint clients**

Use this command to display information about checkpoint clients:

```
Router# show checkpoint clients
```

Check Point List of Clients

CHKPT on ACTIVE server.

Client Name	Client ID	Entity ID	Bundle Mode
-------------	-----------	-----------	-------------

CHKPT Test client	1	--	On
-------------------	---	----	----

Total API Messages Sent:	0
Total IPC Sent:	0
Total Message Len:	0
Total Bytes Allocated:	0
Buffers Held:	0
IPC Frag Count:	0
IPC HW mark:	0
IPC Sends w/Flow Off:	0
Send Errs:	0
Send Peer Errs:	0
Rcv Xform Errs:	0
Xmit Xform Errs:	0
Incompatible Messages:	0

Client Name	Client ID	Entity ID	Bundle Mode
-------------	-----------	-----------	-------------

Network RF Client	3	--	Off
-------------------	---	----	-----

Total API Messages Sent:	10
Total IPC Sent:	10
Total Message Len:	2144
Total Bytes Allocated:	2904
Buffers Held:	0
IPC Frag Count:	0
IPC HW mark:	0
IPC Sends w/Flow Off:	0
Send Errs:	0
Send Peer Errs:	0
Rcv Xform Errs:	0
Xmit Xform Errs:	0
Incompatible Messages:	0

Client Name	Client ID	Entity ID	Bundle Mode
-------------	-----------	-----------	-------------

--More--

.  
.
   
.

**Step 2 show vfi [name vfi-name] checkpoint [summary]**

Use this command to display checkpoint information related to a specific virtual forwarding instance (VFI) named H-VPLS-A-VFI:

```
Router# show vfi name H-VPLS-A-VFI checkpoint
```

```
VFI Active RP
Checkpointing: Allowed
ISSU Client id: 2092, Session id: 65543, Compatible with peer
```

	VFI	VFI AC	VFI PW
Bulk-sync	1	1	3
Checkpoint failures:	0	3	21
Recovered at switchover:	0	0	0
Recovery failures:	0	0	0

Legend: C=Checkpointed

VFI name: H-VPLS-A-VFI, state: up, type: multipoint

VPN ID: 12, Internal ID 1 C

Local attachment circuits:

Vlan200 16387 / 8195 C

Neighbors connected via pseudowires:

Peer ID	VC ID	SSM IDs	
10.0.0.12	12	4096 / 12292	C
10.0.0.15	12	8193 / 16389	C
10.0.0.14	12	12290 / 20486	C

**Step 3 debug cwan atom**

Use this command to enable debugging of Any Transport over MPLS (AToM) platform events.

The following example shows debug message output that appears when debugging is enabled and a PW port is configured and then unconfigured:

```
Router# debug cwan atom
```

ConstWan Generic AToM debugging is on

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# 12 vfi VPLS-2000 manual
```

```
Router(config-vfi)# vpn id 2000
```

```
Router(config-vfi)# neighbor 10.1.1.1 encapsulation mpls
```

```
Router(config-vfi)#
```

```
01:16:36: cwan_rp_vfi_atom_provision_vlan PROV[VFI-ATOM]: plat_index(0xC7D00084)
vlanid(2000) pseudo_port(0x84) vfi_plat_index(0xC7D00084) seginfo(0x53D38220) segtype(25)
seghandle(0x53AEE074) split-horizon(On) cwan_atom_intf(3) vfi_vcs(3) spoke_vcs(0)
```

```
Router(config-vfi)# end
```

```
Router# debug cwan atom
```

ConstWan Generic AToM debugging is on

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# 12 vfi VPLS-2000
```

```
Router(config-vfi)# no neighbor 10.1.1.1 encapsulation mpls
```

```
Router(config-vfi)#
```

```
01:27:18: cwan_rp_vfi_atom_unprovision_vlan: UNPROV[VFI-ATOM]: circ_index(0xC7D00084)
is_vfi(1) vlan(2000) vfi_vcs(3) spoke_vcs(0) split_horizon(On)
```

```
01:27:18: cwan_atom_vlan_remove_rp: Vlan2000 ip_iw(0) ip_enabled(0)
```

```
Router(config-vfi)# end
```

**Step 4 debug cwan ltl**

Use this command to enable debugging of Local Target Manager (LTL) debugging events and errors.

The following example shows debug message outputs that appear when debugging is enabled and a PW port is configured and then unconfigured:

```
Router# debug cwan ltl

ConstWan LTL manager debugging is on
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# 12 vfi VPLS-2000 manual
Router(config-vfi)# vpn id 2000
Router(config-vfi)# neighbor 10.1.1.1 encapsulation mpls
Router(config-vfi)#

01:17:35: CWAN LTL MGR: Port 133 is free to use for VPLS with vlan 2000 - tx_tvc(0x9F404)
Router(config-vfi)# end
Router# debug cwan ltl

ConstWan LTL manager debugging is on
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# 12 vfi VPLS-2000 manual
Router(config-vfi)# no neighbor 10.1.1.1 encapsulation mpls
Router(config-vfi)#

01:29:05: CWAN LTL MGR: DELETE VPLS PW vlan(2000) pseudo_slotunit(133)
Router(config-vfi)# end
```

**Step 5 debug issu client negotiation**

Use this command to enable debugging of ISSU client negotiation events and errors:

```
Router# debug issu client negotiation

*Jun  5 22:41:47.332: VFI ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:41:47.332: ATOM HA: CID 84 Seq 230 Event RF_PROG_STANDBY_CONFIG Op 0 State
ACTIVE Peer STANDBY COLD-CONFIG
*Jun  5 22:41:47.432: ATOM ISSU: Propose L2HW cap 0xFFFF rc 0
*Jun  5 22:41:47.532: ATOM ISSU: Active negotiator, accept compatible L2HW cap 0xFFFF
*Jun  5 22:41:48.232: ATOM ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:41:50.836: cwan_atom_issu_start_nego_session: Start session negotiation
*Jun  5 22:41:50.836: cwan_atom_issu_start_nego_session: Started nego successfully,
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:50.836: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:50.840: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:50.940: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:50.940: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.040: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.040: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.140: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.140: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.240: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:41:51.240: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:41:51.340: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
```



```

*Jun  5 22:50:40.156: VFI ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:50:40.156: ATOM HA: CID 84 Seq 230 Event RF_PROG_STANDBY_CONFIG Op 0 State
ACTIVE Peer STANDBY COLD-CONFIG
*Jun  5 22:50:40.256: ATOM ISSU: Passive negotiator, accept compatible L2HW cap 0xFFF
*Jun  5 22:50:40.964: ATOM ISSU: Negotiation rc ISSU_RC_NEGO_DONE, compatible
*Jun  5 22:50:43.516: cwan_atom_issu_start_nego_session: Start session negotiation
*Jun  5 22:50:43.516: cwan_atom_issu_start_nego_session: Started nego successfully,
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.520: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.520: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.620: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.620: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.720: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.720: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.820: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.820: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:43.920: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0
*Jun  5 22:50:43.920: cwan_atom_issu_receive_nego_msg: issu_receive_nego_msg
rc=ISSU_RC_NEGO_NOT_DONE
*Jun  5 22:50:44.020: cwan_atom_issu_receive_nego_msg: Start, cwan_atom_issu_nego_done=0

```

## Step 6 debug issu client registration

Use this command to enable debugging of ISSU client registration events and errors.

After the peer router reloads, the following debug messages appear:

```
Router# debug issu client registration
```

```
Router#
```

```

00:42:21: VFI ISSU: Unregistered ISSU session 0, ISSU_RC_OK
00:42:21: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed
state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2000, changed state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2001, changed state to down
00:42:21: %LINK-3-UPDOWN: Interface Vlan2002, changed state to down
Router#
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to down
00:42:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to down
Router#
00:49:01: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
00:49:02: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to up
PE-3#
00:49:05: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed
state to up
Router#
00:49:35: %LINK-3-UPDOWN: Interface Vlan2000, changed state to up
00:49:35: %LINK-3-UPDOWN: Interface Vlan2001, changed state to up
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to up
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to up
00:49:35: %LINK-3-UPDOWN: Interface Vlan2002, changed state to up
Router#
00:49:35: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to up
Router#
00:49:48: VFI ISSU: Registered session 131171, ISSU_RC_OK
Router#
00:50:08: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
Router#

```

**Step 7 debug issu client transform [clientID *client-id*]**

Use this command to enable debugging of ISSU client transform events and errors.

The following command example enables debug output for a specific ISSU client (clientID 2092). After the peer router reloads, the following debug messages appear:

```
Router# debug issu client transform clientID 2092

Router#

05:35:15: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet6/2, changed
state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2000, changed state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2001, changed state to down
05:35:15: %LINK-3-UPDOWN: Interface Vlan2002, changed state to down
Router#
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2000, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2001, changed state to down
05:35:15: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2002, changed state to down
Router#
05:41:55: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to down
05:41:56: %LINK-3-UPDOWN: Interface GigabitEthernet6/2, changed state to up
.
.
.
05:43:02: VFI ISSU: Xmit transform message 5, rc ISSU_RC_OK
05:43:02: ISSU Buffer dump @ 0x0817EC7C
05:43:02:      00 00 00 00
05:43:02: VFI ISSU: Xmit transform message 1, rc ISSU_RC_OK
05:43:02: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED succeeded
Router#
```

**Step 8 debug vfi checkpoint**

Use this command to enable debugging VFI checkpointing events and errors:

```
Router# debug vfi checkpoint

Router# $may24_v1 6 slavedisk0:s72033-adventerprisek9_wan-mz.cflow_may24_v1

Router#

*Jun  5 22:37:17.268: ATOM HA: CF status 3 not processed
*Jun  5 22:37:17.268: VFI HA: CF status 3 not processed
*Jun  5 22:37:17.296: AC HA RF: CId:83, Seq:228, Sta:RF_STATUS_PEER_COMM, Opr:0,
St:ACTIVE, PSt:STANDBY HOT
*Jun  5 22:37:17.296: VFI HA: CID 145, Seq 229, Status RF_STATUS_PEER_COMM, Op 0, State
ACTIVE, Peer STANDBY HOT
*Jun  5 22:37:17.296: ATOM HA: CID 84, Seq 230, Status RF_STATUS_PEER_COMM, Op 0, State
ACTIVE, Peer STANDBY HOT
*Jun  5 22:37:17.444: ATOM HA: CF status 3 not processed
*Jun  5 22:37:17.444: VFI HA: CF status 3 not processed
*Jun  5 22:37:17.268: %OIR-SP-3-PWRCYCLE: Card in module 6, is being power-cycled (RF
request)
*Jun  5 22:37:17.792: AC HA RF: CId:83, Seq:228, Sta:RF_STATUS_PEER_PRESENCE, Opr:0,
St:ACTIVE, PSt:DISABLED
*Jun  5 22:37:17.792: VFI HA: CID 145, Seq 229, Status RF_STATUS_PEER_PRESENCE, Op 0,
State ACTIVE, Peer DISABLED
*Jun  5 22:40:40.244: SP-STDBY: SP: Currently running ROMMON from S (Gold) region
*Jun  5 22:40:45.028: %DIAG-SP-STDBY-6-RUN_MINIMUM: Module 6: Running Minimal
Diagnostics...
*Jun  5 22:40:56.492: %DIAG-SP-STDBY-6-DIAG_OK: Module 6: Passed Online Diagnostics
```

```

*Jun  5 22:41:53.436: %SYS-SP-STDBY-5-RESTART: System restarted --
*Jun  5 22:42:12.760: VFI HA: CID 145 Seq 229 Event RF_PROG_STANDBY_BULK Op 0 State ACTIVE
Peer STANDBY COLD-BULK
*Jun  5 22:42:12.764: VFI HA: Ignore RF progression event, VFI Mgr process is not running,
skipped bulk sync
.
.
.
*Jun  5 22:42:16.948: %ISSU_PROCESS-SP-7-DEBUG: Peer state is [ STANDBY HOT ]; Please
issue the runversion command
*Jun  5 22:42:15.928: %PFREDUN-SP-STDBY-6-STANDBY: Ready for SSO mode
*Jun  5 22:42:16.956: %RF-SP-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Jun  5 22:42:16.112: %SYS-SP-STDBY-3-LOGGER_FLUSHED: System was paused for 00:00:00 to
ensure console debugging output.
Router#

```

## Configuration Examples for NSF/SSO/ISSU Support for VPLS

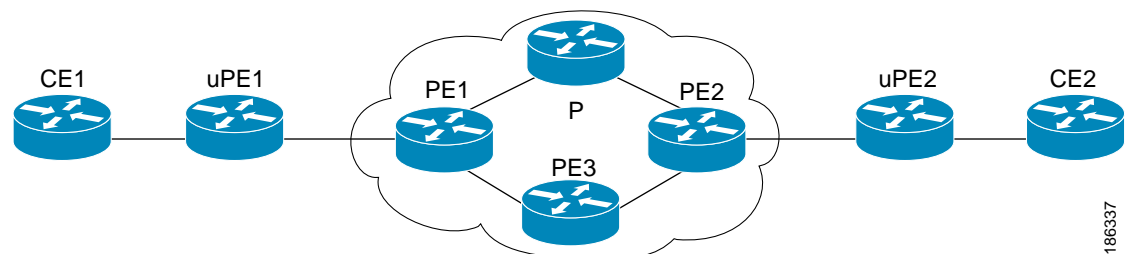
The following example shows the configuration of a network using the NSF/SSO/ISSU Support feature for VPLS:

- [NSF/SSO/ISSU VPLS: Example, page 10](#)

### NSF/SSO/ISSU VPLS: Example

Figure 1 shows a basic configuration of NSF/SSO/ISSU VPLS.

**Figure 1** Basic NSF/SSO/ISSU VPLS Configuration



#### CE1

```

CE1_7206#
!
hostname CE1_7206
!
ip cef
!
interface Loopback0
  description - FULL MESH VPN
  ip address 10.0.0.0 10.255.255.255
!
interface FastEthernet0/0
  ip address 10.0.57.100 255.255.255.0
  no ip mroute-cache
  duplex half
  no cdp enable

```

```

!
interface FastEthernet1/0
  description - H-VPLS VPN to uPE1
  no ip address
  no ip mroute-cache
  duplex auto
  speed auto
!
interface FastEthernet1/0.1
  description - H-VPLS VPN to uPE1
  encapsulation dot1Q 121
  ip address 10.1.1.120 255.255.255.0
!
interface FastEthernet4/1
  description - FULL MESH VPN to PE1
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet4/1.1
  description - FULL MESH VPN to PE1
  encapsulation dot1Q 120
  ip address 10.1.1.120 255.255.255.0
!
interface FastEthernet6/1
  description - VPWS VPN to PE1
  no ip address
  duplex auto
  speed auto
!
interface FastEthernet6/1.1
  description - VPWS VPN to PE1
  encapsulation dot1Q 122
  ip address 10.1.1.120 255.255.255.0
!
router ospf 10
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 10.120.120.120 0.0.0.0 area 0
  network 10.1.1.0 0.0.0.255 area 0
!
ip default-gateway 10.0.57.1
!
end

```

## uPE1

```

uPE1_7609#
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
!
hostname uPE1_7609
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
no aaa new-model

```

```

!
no ip domain lookup
ip host lab24 172.16.0.0
ip host dirt 172.16.0.19
!
vtp mode transparent
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
redundancy
  mode sso
  main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
vlan 100
!
interface Loopback0
  description - H-VPLS
  ip address 10.0.0.0 255.255.255.255
!
interface GigabitEthernet1/1
  description - H-VPLS to CE1
  switchport
  switchport trunk allowed vlan 10-1000
  switchport mode trunk
!
interface GigabitEthernet5/2
  ip address 10.0.0.0 255.255.255.0
  media-type rj45
  no cdp enable
!
interface GigabitEthernet9/0/0
  description - H-VPLS to PE1
  ip address 10.0.0.1 255.255.255.0
  negotiation auto
  mpls label protocol ldp
  mpls ip
!
interface Vlan1
  no ip address
  shutdown
!
router ospf 10
  log-adjacency-changes
  passive-interface Loopback0
  network 10.0.5.0 0.0.0.255 area 0
  network 10.0.0.8 0.0.0.0 area 0
!
ip route 172.16.17.19 255.255.255.255 10.0.57.1
ip route 172.16.0.0 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!

```

```
control-plane
!  
end
```

## PE1

```
PE1_7613#  
!  
upgrade fpd auto  
service internal  
!  
hostname PE1_7613  
!  
boot-start-marker  
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xxx  
boot-end-marker  
!  
no aaa new-model  
ip subnet-zero  
!  
!  
no ip domain lookup  
ip host dirt 172.16.0.0  
ip host lab24 172.16.0.01  
!  
ipv6 mfib hardware-switching replication-mode ingress  
!  
mls ip multicast flow-stat-timer 9  
no mls flow ip  
no mls flow ipv6  
no mls acl tcam share-global  
mls cef error action freeze  
multilink bundle-name authenticated  
mpls ldp discovery targeted-hello accept  
mpls label protocol ldp  
!  
!  
spanning-tree mode pvst  
no spanning-tree optimize bpdu transmission  
spanning-tree extend system-id  
!  
redundancy  
  mode sso  
  main-cpu  
    auto-sync running-config  
!  
vlan internal allocation policy ascending  
vlan dot1q tag native  
vlan access-log ratelimit 2000  
12 vfi vpls_auto autodiscovery  
  vpn id 1  
!  
12 vfi vpls_man manual  
  vpn id 10  
  neighbor 10.0.0.12 encapsulation mpls  
  neighbor 10.0.0.11 encapsulation mpls  
!  
interface Loopback0  
  description - FULL MESH  
  ip address 10.0.0.9 255.255.255.255  
!  
interface Loopback1  
  description - VPWS
```

```

ip address 172.16.0.0 255.255.255.255
!
interface Loopback2
description - H-VPLS
ip address 10.0.0.0 255.255.255.255
!
interface GigabitEthernet7/2
ip address 10.0.0.01 255.255.255.0
media-type rj45
no cdp enable
!
interface GigabitEthernet10/1
description - FULL MESH to CE1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-1000
switchport mode trunk
!
interface GigabitEthernet10/2
description - VPWS to CE1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-1000
switchport mode trunk
!
interface GigabitEthernet12/0/0
description - H-VPLS to uPE1
ip address 10.0.0.3 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet12/0/1
description - H-VPLS to nPE2
ip address 10.0.0.1 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet12/1/0
description - VPWS to P
ip address 10.0.0.3 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet12/1/1
description - FULL MESH to P
ip address 10.0.2.0 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet12/2/0
description - FULL MESH to PE3
ip address 10.1.0.3 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface Vlan1
no ip address
shutdown
!

```

```

interface Vlan10
  no ip address
  xconnect vfi vpls_auto
!
router ospf 10
  ! for FULL MESH
  log-adjacency-changes
  passive-interface Loopback0
  network 10.1.1.0 0.0.0.255 area 0
  network 10.2.2.0 0.0.0.255 area 0
  network 10.5.5.0 0.0.0.255 area 0
  network 10.9.9.9 0.0.0.0 area 0
  network 10.0.0.02 0.0.0.255 area 0
  network 10.0.0.04 0.0.0.0 area 0
  network 10.0.0.5 0.0.0.0 area 0
!
router ospf 20
  ! for VPWS
  log-adjacency-changes
  passive-interface Loopback1
  network 10.0.20.0 0.0.0.255 area 0
  network 10.0.0.9 0.0.0.0 area 0
!
router bgp 1
  bgp log-neighbor-changes
  neighbor 10.0.11.0 remote-as 1
  neighbor 10.0.10.0 update-source Loopback0
  neighbor 10.0.12.0 remote-as 1
  neighbor 10.0.0.12 update-source Loopback0
  neighbor 10.0.0.32 remote-as 1
  neighbor 10.0.0.31 update-source Loopback2
!
  address-family ipv4
    no synchronization
    neighbor 10.0.11.0 activate
    neighbor 10.12.0.0 activate
    neighbor 10.0.32.0 activate
    no auto-summary
  exit-address-family
!
  address-family l2vpn vpls
    neighbor 10.0.0.11 activate
    neighbor 10.0.11.0 send-community both
    neighbor 10.12.0.0 activate
    neighbor 10.0.0.12 send-community both
    neighbor 10.0.0.32 activate
    neighbor 10.0.32.0 send-community both
  exit-address-family
!
  ip default-gateway 10.0.57.1
  ip route 172.16.0.0 255.255.255.255 10.0.57.1
  ip route 172.16.0.2 255.255.255.255 10.0.57.1
!
  mpls ldp router-id Loopback0 force
!
end

```

## P

```

P_7206_g1#
!
version 12.4
service timestamps debug datetime msec

```



```

service timestamps log datetime msec
no service password-encryption
!
hostname P_7206_g1
!
ip cef
ip host lab24 172.16.0.254
ip host dirt 172.16.0.129
!
mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
!
interface Loopback0
description - FULL MESH
ip address 10.0.0.10 255.255.255.255
!
interface Loopback1
description - VPWS
ip address 10.0.0.1 255.255.255.255
!
!
interface GigabitEthernet1/0
description - VPWS to PE1
ip address 10.0.20.6 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet2/0
description - FULL MESH to PE1
ip address 10.0.2.6 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet3/0
description - VPWS to PE2
ip address 10.0.0.6 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet4/0
description - FULL MESH to PE2
ip address 10.0.3.6 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
router ospf 10
! for FULL MESH
log-adjacency-changes
passive-interface Loopback0
network 10.0.2.6 0.0.0.0 area 0
network 10.0.2.0 0.0.0.255 area 0
network 10.0.3.6 0.0.0.0 area 0
network 10.0.3.0 0.0.0.255 area 0
network 10.0.0.0 0.0.0.255 area 0
!
router ospf 20
! for VPWS
log-adjacency-changes
passive-interface Loopback1

```

```

network 10.0.20.0 0.0.0.255 area 0
network 10.21.0.0 0.0.0.255 area 0
network 10.0.10.0 0.0.0.0 area 0
!
router bgp 1
no synchronization
bgp log-neighbor-changes
neighbor 10.0.9.9 remote-as 1
neighbor 10.9.0.9 update-source Loopback0
neighbor 10.11.0.11 remote-as 1
neighbor 10.0.11.0 update-source Loopback0
no auto-summary
!
ip default-gateway 10.0.0.0
!
mpls ldp router-id Loopback0 force
!

```

## PE2

```

PE2_7606#
!
upgrade fpd auto
!
service internal
service counters max age 10
!
hostname PE2_7606
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
no aaa new-model
!
ipv6 mfib hardware-switching replication-mode ingress
!
mls ip multicast flow-stat-timer 9
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
redundancy
mode sso
main-cpu
auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
l2 vfi vpls_auto autodiscovery
vpn id 1
!
l2 vfi vpls_manual manual

```

```

vpn id 10
neighbor 10.0.0.9 encapsulation mpls
neighbor 10.0.0.11 encapsulation mpls
!
interface Loopback0
description - FULL MESH
ip address 10.0.0.12 255.255.255.255
!
interface Loopback1
description - VPWS
ip address 10.0.0.112 255.255.255.255
!
interface Loopback2
description - H-VPLS
ip address 10.0.32.0 255.255.255.255
!
interface GigabitEthernet2/1
description - FULL MESH to CE2
switchport
switchport trunk allowed vlan 10-1000
switchport mode trunk
!
interface GigabitEthernet4/0/0
description - FULL MESH to PE3
ip address 10.0.4.0 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet4/1/0
description - VPWS to P
ip address 10.0.21.0 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet4/1/1
description - FULL MESH to P
ip address 10.0.3.4 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet4/3/0
description - VPWS to CE2
no ip address
shutdown
negotiation auto
!
interface GigabitEthernet4/3/1
description - H-VPLS to nPE1
ip address 10.0.0.3 255.255.255.0
negotiation auto
mpls label protocol ldp
mpls ip
!
interface GigabitEthernet5/2
ip address 10.0.5.0 255.255.255.0
media-type rj45
no cdp enable
!
interface Vlan1
no ip address
shutdown

```

```

!
interface Vlan10
 no ip address
 shutdown
 xconnect vfi vpls_auto
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.3.4 0.0.0.0 area 0
 network 10.0.4.0 0.0.0.255 area 0
 network 10.0.6.4 0.0.0.0 area 0
 network 10.0.0.5 0.0.0.255 area 0
 network 10.0.0.12 0.0.0.0 area 0
 network 10.0.32.0 0.0.0.0 area 0
 network 10.0.1.0 0.0.0.0 area 0
!
router bgp 1
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.0.0.9 remote-as 1
 neighbor 10.0.9.0 update-source Loopback0
 neighbor 10.0.11.0 remote-as 1
 neighbor 10.0.0.11 update-source Loopback0
 neighbor 10.0.29.0 remote-as 1
 neighbor 10.0.0.29 update-source Loopback2
!
 address-family ipv4
  no synchronization
  no auto-summary
 exit-address-family
!
 address-family l2vpn vpls
  neighbor 10.0.0.9 activate
  neighbor 10.0.9.0 send-community both
  neighbor 10.0.11.0 activate
  neighbor 10.0.0.11 send-community both
  neighbor 10.0.0.2 activate
  neighbor 10.0.0.3 send-community both
 exit-address-family
!
 ip default-gateway 10.0.0.1
 ip route 172.16.0.0 255.255.255.255 10.0.57.1
 ip route 172.16.0.254 255.255.255.255 10.0.57.1
!
 mpls ldp router-id Loopback0 force
!
end

```

## uPE2

```

uPE2_7606#
!
 upgrade fpd auto
 version 12.2
 service timestamps debug uptime
 service timestamps log uptime
 service internal
!
 hostname uPE2_7606
!
 boot-start-marker

```

```

boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
ipv6 mfib hardware-switching replication-mode ingress
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
power redundancy-mode combined
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
!
interface Loopback0
 description - H-VPLS
 ip address 10.0.0.13 255.255.255.255
!
interface FastEthernet3/1
 description - H-VPLS to CE2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10-1000
 switchport mode trunk
!
interface GigabitEthernet4/0/0
 description - H-VPLS to uPE2
 ip address 10.0.0.2 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet5/2
 ip address 10.0.0.11 255.255.255.0
 media-type rj45
 no cdp enable
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 10
 log-adjacency-changes
 passive-interface Loopback0
 network 10.0.6.0 0.0.0.255 area 0
 network 10.0.0.13 0.0.0.0 area 0
!
ip default-gateway 10.0.0.1
ip route 172.16.1.129 255.255.255.255 10.0.57.1
ip route 172.16.192.254 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!

```

```
control-plane
!  
end
```

## CE2

```
CE2_7206#  
!  
hostname CE2_7206  
!  
ip cef  
!  
interface Loopback0  
  ip address 10.0.0.123 255.255.255.255  
!  
interface FastEthernet1/0  
  description - H-VPLS VPN to uPE2  
  no ip address  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
interface FastEthernet1/0.1  
  description - H-VPLS VPN to uPE2  
  encapsulation dot1Q 10  
  ip address 10.0.0.121 255.255.255.0  
!  
interface Ethernet2/0  
  ip address 10.0.0.97 255.255.255.0  
  no ip mroute-cache  
  duplex half  
  no cdp enable  
!  
interface FastEthernet4/0  
  description - FULL MESH VPN to PE2  
  no ip address  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
interface FastEthernet4/0.1  
  description - FULL MESH VPN to PE2  
  encapsulation dot1Q 10  
  ip address 10.0.0.121 255.255.255.0  
!  
interface GigabitEthernet5/0  
  description - VPWS VPN to PE2  
  no ip address  
  no ip mroute-cache  
  no negotiation auto  
!  
interface GigabitEthernet5/0.1  
  description - VPWS VPN to PE2  
  encapsulation dot1Q 10  
  ip address 10.0.0.121 255.255.255.0  
!  
router ospf 10  
  log-adjacency-changes  
  network 10.0.1.0 0.0.0.255 area 0  
  network 10.0.0.1 0.0.0.255 area 0  
  network 10.0.0.123 0.0.0.0 area 0  
!  
ip default-gateway 10.0.0.4
```

```
!
end
```

### PE3

```
PE3_7606#
!
upgrade fpd auto
version 12.2
service timestamps debug uptime
service timestamps log uptime
service internal
!
hostname PE3_7606
!
boot-start-marker
boot system flash disk0:s72033-adventerprisek9_wan_dbg-mz.xx
boot-end-marker
!
ipv6 mfib hardware-switching replication-mode ingress
!
multilink bundle-name authenticated
mpls ldp graceful-restart
mpls ldp discovery targeted-hello accept
mpls label protocol ldp
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
redundancy
 mode sso
 main-cpu
  auto-sync running-config
!
vlan internal allocation policy ascending
vlan dot1q tag native
vlan access-log ratelimit 2000
l2 vfi vpls_auto autodiscovery
  vpn id 1
!
l2 vfi vpls_manual manual
  vpn id 10
  neighbor 10.0.9.9 encapsulation mpls
  neighbor 10.0.0.12 encapsulation mpls
!
interface Loopback0
 description - FULL MESH
 ip address 10.0.0.11 255.255.255.255
!
interface Loopback1
 description - H-VPLS
 ip address 10.0.0.31 255.255.255.255
!
interface GigabitEthernet3/2/1
 description - FULL MESH to PE1
 ip address 10.0.0.5 255.255.255.0
 negotiation auto
 mpls label protocol ldp
 mpls ip
!
interface GigabitEthernet5/2
 ip address 10.0.0.115 255.255.255.0
```

```
media-type rj45
no cdp enable
!
interface GigabitEthernet6/2
description - FULL MESH to CE3
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 10-1000
switchport mode trunk
no cdp enable
!
interface Vlan1
no ip address
shutdown
!
router ospf 10
log-adjacency-changes
passive-interface Loopback0
network 10.0.4.0 0.0.0.255 area 0
network 10.0.0.11 0.0.0.0 area 0
network 10.0.31.0 0.0.0.0 area 0
!
router bgp 1
no bgp default ipv4-unicast
bgp log-neighbor-changes
bgp update-delay 1
neighbor 10.0.0.9 remote-as 1
neighbor 10.0.9.0 update-source Loopback0
neighbor 10.0.12.0 remote-as 1
neighbor 10.0.0.12 update-source Loopback0
!
address-family ipv4
no synchronization
no auto-summary
exit-address-family
!
address-family l2vpn vpls
neighbor 10.0.9.0 activate
neighbor 10.0.0.9 send-community both
neighbor 10.0.0.12 activate
neighbor 10.0.12.0 send-community both
exit-address-family
!
ip default-gateway 10.0.57.1
ip route 172.16.0.129 255.255.255.255 10.0.57.1
ip route 172.16.0.254 255.255.255.255 10.0.57.1
!
mpls ldp router-id Loopback0 force
!
end
```



# Additional References

The following sections provide references related to the NSF/SSO/ISSU Support for VPLS feature.

## Related Documents

Related Topic	Document Title
Stateful switchover	<a href="#">Stateful Switchover</a>
MPLS Label Distribution Protocol	<a href="#">MPLS Label Distribution Protocol (LDP)</a>
Cisco nonstop forwarding	<a href="#">Cisco Nonstop Forwarding</a>
Any Transport over MPLS	<a href="#">Any Transport over MPLS</a>
NSF/SSO: Any Transport over MPLS	<a href="#">NSF/SSO—Any Transport over MPLS and AToM Graceful Restart</a>
L2VPN Interworking configuration	<a href="#">L2VPN Interworking</a>
VPLS	See the “Virtual Private LAN Services on the Optical Services Modules” chapter in the <a href="#">Cisco 7600 Series Router Cisco IOS Software Configuration Guide</a> , Release 12.2SR)
VPLS Autodiscovery	See <a href="#">VPLS Autodiscovery: BGP Based</a> and <a href="#">BGP Support for the L2VPN Address Family</a>
NSF/SSO router support on the 7600 router	See the “Configuring NSF with SSO Supervisor Engine Redundancy” chapter in the <a href="#">Cisco 7600 Series Cisco IOS Software Configuration Guide</a> , Release 12.2SR
ISSU router support on the 7600 router	See the “ISSU and eFSU on Cisco 7600 Series Routers” chapter in the <a href="#">Cisco 7600 Series Cisco IOS Software Configuration Guide</a> , Release 12.2SR

## Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
MPLS Label Distribution Protocol MIB Version 8 Upgrade	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 3036	<i>LDP Specification</i>
RFC 3478	<i>Graceful Restart Mechanism for Label Distribution</i>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at [http://www.cisco.com/en/US/docs/ios/mps/command/reference/mp\\_book.html](http://www.cisco.com/en/US/docs/ios/mps/command/reference/mp_book.html). For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

- **debug cwan atom**
- **debug cwan ltl**
- **debug issu client negotiation**
- **debug issu client registration**
- **debug issu client transform**
- **debug vfi checkpoint**
- **show checkpoint clients**
- **show vfi checkpoint**

# Feature Information for NSF/SSO/ISSU Support for VPLS

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for NSF/SSO/ISSU Support for VPLS

Feature Name	Releases	Feature Information
NSF/SSO/ISSU Support for VPLS	12.2(33)SRC	Virtual Private LAN Services (VPLS), with NSF/SSO/ISSU support, improves the availability of service provider networks that use VPLS for multipoint Layer 2 VPN services. Cisco nonstop forwarding (NSF) with stateful switchover (SSO) is effective at increasing availability of network services.  In 12.2(33)SRC, this feature was introduced on the Cisco 7600 router.

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

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

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

© 2008 Cisco Systems, Inc. All rights reserved.



# NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

---

**First Published: October 21, 2009**

**Last Updated: November 25, 2009**

This document provides information about configuring nonstop forwarding (NSF), stateful switchover (SSO), and In Service Software Upgrade (ISSU) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) and Cisco IOS IPv6 provider edge router (6PE) over Multiprotocol Label Switching (MPLS).

## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE”](#) section on [page 17](#).

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

## Contents

- [Prerequisites for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 2](#)
- [Restrictions for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 2](#)
- [Information About NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 2](#)
- [How to Configure NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 6](#)
- [Configuration Examples for Configuring NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 12](#)
- [Additional References, page 15](#)
- [Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 17](#)
- [Glossary, page 19](#)



---

**Americas Headquarters:**

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

## Prerequisites for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

Ensure that the following are supported for the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature to work:

- IPv6 NSF
- IPv6 Cisco Express Forwarding
- Label Distribution Protocol (LDP) Graceful Restart

LDP Graceful Restart should be enabled if LDP is the protocol used in the MPLS core

You must enable NSF on the following routing protocol that run between the provider (P) routers, PE routers, and the customer edge (CE) routers:

- Border Gateway Protocol (BGP)
- Static routes

Before enabling the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature, you must have a supported MPLS VPN network configuration. See the configuration information included in the following modules: [Configuring MPLS Layer 3 VPNs](#), [Implementing IPv6 over MPLS](#), and [Implementing IPv6 VPN over MPLS](#).

## Restrictions for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

The NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature has the following restrictions:

- Tag Distribution Protocol (TDP) sessions are not supported. Only LDP sessions are supported.
- MPLS VPN 6VPE and 6PE Carrier Supporting Carrier (CSC) VPNs support only BGP. CSC configurations that use LDP are not supported.
- Only BGP and static routes are supported for 6VPE and 6PE in Cisco IOS Release 12.2(33)SRE.

## Information About NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

To configure the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature, you need to understand the following concepts:

- [Elements Supporting NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE Features, page 3](#)
- [How BGP Graceful Restart Works for MPLS VPN 6VPE and 6PE, page 3](#)
- [How BGP Graceful Restart Preserves Prefix Information During a Restart, page 3](#)
- [ISSU Support for MPLS VPN 6VPE and 6PE, page 4](#)
- [NSF/SSO Support for MPLS VPN 6VPE and 6PE, page 4](#)
- [BGP Graceful Restart Support for MPLS VPN Configurations, page 5](#)
- [What Happens If a Router Does Not Support NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE, page 5](#)

## Elements Supporting NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE Features

The major elements supporting the functionality of the NSF/SSO and ISSU for Cisco IOS VPN 6vPE and 6PE feature are the following:

- **MPLS VPN**—A supported MPLS VPN network must be configured before you enable the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature
- **BGP Graceful Restart**—The BGP Graceful Restart feature is responsible for negotiating graceful restart capabilities, exchanging forwarding preservation states, and coordinating advertisements after session restarts. MPLS VPNs interact with BGP to exchange Virtual Private Network (VPN) routing and forwarding (VRF) routes and labels.
- **IPv6 NSF**—IPv6 NSF support enables IPv6 cache rebuilds during switchover using checkpointed Cisco Express Forwarding adjacencies.
- **CEF/MFI**—Cisco Express Forwarding and the MPLS Forwarding Infrastructure are responsible for preserving forwarding entries and local labels across Route Processor (RP) switchover.

## How BGP Graceful Restart Works for MPLS VPN 6vPE and 6PE

BGP Graceful Restart behavior for IPv6 and VPNv6 is essentially the same as Graceful Restart behavior for IPv4 and VPNv4; the only difference is the addition of support for IPv6 and VPNv6 address families.

When you configure BGP Graceful Restart, BGP includes the Graceful Restart capability and negotiates the preservation states of address families, that is, IPv4/VPNv4 and IPv6/VPNv6 address families.

Both BGP peers must agree on a Graceful Restart timer, which you can set with the **bgp graceful-restart restart-timer seconds** command. After a BGP session comes up and finishes sending initial updates, each BGP peer sends an end-of-Routing Information Base (RIB) marker.

The NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature uses the mechanisms defined in the RFC 4724, *Graceful Restart Mechanism for BGP*, and in the *Cisco Nonstop Forwarding* feature module.

## How BGP Graceful Restart Preserves Prefix Information During a Restart

When a router that is capable of BGP Graceful Restart loses connectivity, the following happens to the restarting router:

1. The router establishes BGP sessions with other routers and relearns the BGP routes from other routers that are also capable of Graceful Restart. The restarting router waits to receive updates from the neighboring routers. When the neighboring routers send end-of-RIB markers to indicate that they are done sending updates, the restarting router starts sending its own updates.
2. The restarting router recovers labels from the MPLS Forwarding Infrastructure (MFI) database for each prefix. If the router finds the label, it advertises the label to the neighboring router. If the router does not find the label, it allocates a new label from the database and advertises it.
3. The restarting router removes any stale prefixes after a timer for stale entries expires.

When a peer router that is capable of BGP Graceful Restart encounters a restarting router, it does the following:

1. The peer router sends all of the routing updates to the restarting router. When it has finished sending updates, the peer router sends an end-of RIB marker to the restarting router.

2. The peer router does not immediately remove the BGP routes learned from the restarting router from its BGP routing table. As it learns the prefixes from the restarting router, the peer refreshes the stale routes if the new prefix and label information matches the old information.

## ISSU Support for MPLS VPN 6vPE and 6PE

In Cisco IOS Release 12.2(33)SRE and future releases, ISSU supports MPLS VPN 6vPE and 6PE. The Cisco IOS ISSU process allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

ISSU support for MPLS 6vPE and 6PE relies on 6vPE and 6PE NSF/SSO capability on the platform to minimize disruption on the forwarding plane.

For more information about ISSU, see [Cisco IOS In Service Software Upgrade Process](#).

## NSF/SSO Support for MPLS VPN 6VPE and 6PE

In Cisco IOS Release 12.2(33)SRE and future releases, NSF/SSO supports MPLS VPN 6vPE and 6PE. NSF/SSO for 6VPE and 6PE supports the following configurations:

- NSF/SSO for IPv4 and VPNv4 coexistence
- Basic 6VPE and 6PE over MPLS core technology
- BGP multipath configuration

NSF/SSO for 6VPE supports the following configurations:

- Per-VRF label configuration
- Inter autonomous systems (Inter-AS) topologies, including options B and C
- CSC when IPv6 + labels is configured on the PE-customer edge (CE) link

Because the SSO feature maintains stateful protocol and application information, user session information is maintained during a switchover, and line cards continue to forward network traffic with no loss of sessions, providing improved network availability. SSO initializes and configures the standby RP and synchronizes state information, which can reduce the time required for routing protocols to converge. Network stability may be improved with the reduction in the number of route flaps created when routers in the network failed and lost their routing tables.

When RP switchover happens, forwarding information is preserved by MFI and Cisco Express Forwarding on both line cards and the standby RP. VPNv6 prefix and local label mapping is preserved in the forwarding database. When the standby RP becomes the new active RP, 6PE and 6vPE traffic continues to be forwarded with minimal interruption.

When a BGP session restarts on the new active RP, the new active RP does not have any prior state information about prefixes or labels. The new active RP will have to relearn VPNv6 prefixes from its peers. As the new active RP learns the VPNv6 prefixes, it tries to get new local labels the same way it does when it first comes up. If the MFI database has the preserved copy of the local label for a prefix, the MFI database gives the local label to BGP. Then, BGP maintains the same local label. If the MFI database does not have a preserved local label for the prefix, MFI allocates a new one.

## BGP Graceful Restart Support for MPLS VPN Configurations

The section describes BGP Graceful Restart support for a basic 6VPE setup and for a CSC setup and interautonomous system setup.

- [Graceful Restart Support for a Basic 6VPE Setup, page 5](#)
- [Graceful Restart for 6VPE in Carrier Supporting Carrier and Interautonomous System Setups, page 5](#)

### Graceful Restart Support for a Basic 6VPE Setup

For PE- to-CE external BGP (eBGP), Graceful Restart capability is supported for IPv6 address families. For PE-to-PE interior BGP (iBGP) sessions with or without a route reflector (RR) in the core, BGP Graceful Restart capability supports VPNv6 address families.

When the PE router resets, the connected CE router retains IPv6 prefixes that it received from the PE router and marks the prefixes as stale. If the eBGP session does not reestablish within the specified restart time or the session reestablishes, but does not set the restart or forwarding state bit, the CE router removes the staled IPv6 routes. If the eBGP session reestablishes within the specified restart time and has both the forwarding and restart bits set, the CE router removes the stale state from the IPv6 routes when it receives the updates from PE router. After the CE router receives the end-of-RIB marker, it removes or withdraws the rest of the staled information, if any exists.

The restarting PE router waits for an end-of-RIB marker from all BGP-capable peers including iBGP peers and eBGP peers. Only after receiving an end-of-RIB marker from all BGP capable peers will the PE router start to calculate the best path and send out initial updates.

### Graceful Restart for 6VPE in Carrier Supporting Carrier and Interautonomous System Setups

The same Graceful Restart capabilities for route preservation that apply to a basic 6VPE setup apply to a CSC and Inter-AS setup. IPv6 or VPNv6 routes and labels are preserved during switchover.

In a CSC configuration, when send-labels are configured between a CSC-PE and CSC-CE eBGP connection, labels are preserved along with IPv6 BGP routes when one of the peers restarts.

In Inter-AS option B and options C setups, VPNv6 routes and labels are preserved on an Autonomous System Border Router (ASBR) or route reflector when the VPNv6 peer restarts.

## What Happens If a Router Does Not Support NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

If a router does not support the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature, prefix and label information is not preserved. After a switchover, BGP has to restart, relearn all routes, and install labels in the forwarding database. This might result in the loss of some network traffic.



# How to Configure NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

Perform the following tasks to configure NSF/SSO for MPLS 6VPE and 6PE:

- [Configuring NSF/SSO for Basic MPLS 6VPEs and 6PEs, page 6](#) (required)
- [Verifying NSF/SSO and ISSU Support for MPLS VPN 6VPE and 6PE, page 8](#) (optional)

For information on how to configure ISSU, see the [Cisco IOS In Service Software Upgrade Process](#) module.

## Configuring NSF/SSO for Basic MPLS 6VPEs and 6PEs

Perform this task to configure NSF/SSO for basic MPLS 6VPE and 6PEs.



### Note

You can use the **bgp graceful-restart** command to configure BGP Graceful Restart for all available address families.

## Prerequisites

Route Processors must be configured for SSO. See [Stateful Switchover](#) for more information.

If you use LDP in the core, you must enable the MPLS LDP: NSF/SSO Support and Graceful Restart feature. See [NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart](#) for more information.

You must enable nonstop forwarding on the routing protocols running between the P, PE, and CE routers. The routing protocols between the CE router and the PE router are Static and BGP. See [Cisco Nonstop Forwarding](#) for more information.

Before enabling the NSF/SSO—MPLS VPN feature, you must have a supported MPLS VPN network configuration. See configuration information included in the following: [Configuring MPLS Layer 3 VPNs](#), [Implementing IPv6 over MPLS](#), and [Implementing IPv6 VPN over MPLS](#).

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **ipv6 unicast-routing**
5. **ipv6 cef distributed**
6. **redundancy**
7. **mode sso**
8. **exit**
9. **router bgp** *autonomous-system-number*
10. **bgp graceful-restart restart-time** *seconds*
11. **bgp graceful-restart stalepath-time** *seconds*
12. **bgp graceful-restart**
13. **end**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip cef distributed</b>  <b>Example:</b> Router(config)# ip cef distributed	Enables distributed Cisco Express Forwarding.
Step 4	<b>ipv6 unicast-routing</b>  <b>Example:</b> Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
Step 5	<b>ipv6 cef distributed</b>  <b>Example:</b> Router(config)# ipv6 cef distributed	Enables distributed Cisco Express Forwarding for IPv6.
Step 6	<b>redundancy</b>  <b>Example:</b> Router(config)# redundancy	Enters redundancy configuration mode.
Step 7	<b>mode sso</b>  <b>Example:</b> Router(red-config)# mode sso	Sets the redundancy configuration mode to SSO.
Step 8	<b>exit</b>  <b>Example:</b> Router(red-config)# exit	Exits to global configuration mode.
Step 9	<b>router bgp autonomous-system-number</b>  <b>Example:</b> Router(config)# router bgp 1000	Enters router configuration mode and configures the BGP routing process. <ul style="list-style-type: none"> <li>The <i>autonomous-system-number</i> argument is the number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number is in the range from 1 to 65535.</li> </ul>

	Command or Action	Purpose
Step 10	<b>Command:</b> <code>bgp graceful-restart restart-time seconds</code>  <b>Example:</b> <pre>Router(config-router)# bgp graceful-restart restart-time 180</pre>	Enables the BGP graceful restart timer capability globally for all BGP neighbors. <ul style="list-style-type: none"> <li>The <b>restart-time seconds</b> keyword and argument sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for the <i>seconds</i> argument is 120. The configurable range of values is from 1 to 3600.</li> </ul>
Step 11	<b>Command:</b> <code>bgp graceful-restart stalepath-time seconds</code>  <b>Example:</b> <pre>Router(config-router)# bgp graceful-restart stalepath-time 420</pre>	Enables the BGP graceful restart stale path timer capability globally for all BGP neighbors. <ul style="list-style-type: none"> <li>The <b>stalepath-time seconds</b> keyword and argument sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for the <i>seconds</i> argument is 360. The configurable range of values is from 1 to 3600.</li> </ul>
Step 12	<b>Command:</b> <code>bgp graceful-restart</code>  <b>Example:</b> <pre>Router(config-router)# bgp graceful-restart</pre>	Enables the BGP graceful restart capability globally for all BGP neighbors.
Step 13	<b>Command:</b> <code>end</code>  <b>Example:</b> <pre>Router(config-router)# end</pre>	Exits to privileged EXEC mode.

## Verifying NSF/SSO and ISSU Support for MPLS VPN 6VPE and 6PE

Perform this task to verify NSF/SSO and ISSU support for 6VPE and 6PE.

### SUMMARY STEPS

1. `enable`
2. `show ip bgp neighbor`
3. `show ip bgp vpnv6 unicast vrf vrf-name`
4. `show ip bgp ipv6 unicast`
5. `show mpls forwarding`
6. `show ipv6 cef vrf-name`

### DETAILED STEPS

- |               |   |
|---------------|---|
| <b>Step 1</b> | <b>enable</b><br><br>Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:<br><br><pre>Router&gt; enable Router#</pre> |
|---------------|---|

**Step 2** **show ip bgp neighbor**

Use this command to verify that the IPv6 address family and VPNv6 address family entries are preserved. For example:

```
Router# show ip bgp neighbor
```

```
BGP neighbor is 10.2.2.2, remote AS 100, internal link
  BGP version 4, remote router ID 10.2.2.2
  BGP state = Established, up for 00:02:42
  Last read 00:00:36, last write 00:00:36, hold time is 180, keepalive
.
.
.
  Neighbor capabilities:
.
.
.
  Graceful Restart Capability: advertised and received
    Remote Restart timer is 120 seconds
  Address families advertised by peer:
    IPv6 Unicast (was preserved), VPNv6 Unicast (was preserved)
```

IPv6 Unicast (was preserved), VPNv6 Unicast (was preserved) is displayed in the Graceful Restart Capability section of the output only after the peer restarts.

**Step 3** **show ip bgp vpnv6 unicast vrf vrf-name**

Use this command to verify that VPNv6 entries are marked as staled during switchover. For example:

```
Router# show ip bgp vpnv6 unicast vrf vpn1
```

```
BGP table version is 10, local router ID is 10.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
S>iA::1/128       ::FFFF:10.2.2.2      0      100      0 200 ?
*> A::5/128       A::4:5:5             0              0 200 ?
S>iA::1:2:0/112   ::FFFF:10.2.2.2      0      100      0 ?
* A::4:5:0/112   A::4:5:5             0              0 200 ?
```

**Step 4** **show ip bgp ipv6 unicast**

Use this command to verify that VPNv6 entries are marked as staled during switchover. For example:

```
Router# show ip bgp ipv6 unicast
```

```
BGP table version is 9, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop          Metric LocPrf Weight Path
*> A::1/128       ::              0          32768 ?
S A::1:2:0/112   A::1:2:2        0              0 100 ?
*>               ::              0          32768 ?
S> A::4:5:0/112   A::1:2:2        0              0 100 ?
Router#
```

**Step 5 show mpls forwarding**

Use this command to show preserved forwarding entries for IPv6 and VPNv6 prefixes. The sample output is from a PE router in a CSC configuration. Enter the command on the active and the standby router. Compare the sample output from the active router with the sample output from the standby router. Following is sample output from the active router;

Router# **show mpls forwarding**

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
18	Pop Label	10.3.3.3/32	0		Et1/0	10.2.3.3
19	Pop Label	10.3.4.0/24	0		Et1/0	10.2.3.3
20	17	10.4.4.4/32	0		Et1/0	10.2.3.3
21	Pop Label	10.1.2.1/32[V]	0		Et0/0	10.1.2.1
22	Pop Label	A::1:2:0/112[V]	0		aggregate/vpn1	
23	Pop Label	A::1:2:1/128[V]	0		Et0/0	A::1:2:1
24	Pop Label	10.1.2.0/24[V]	0		aggregate/vpn1	
25	Pop Label	A::1:2:2/128[V]	0		aggregate/vpn1	
26	18	A::1/128[V]	0		Et0/0	
FE80::A8BB:CCFF:FE03:2101						
27	26	10.4.5.5/32[V]	0		Et1/0	10.2.3.3
28	25	10.4.5.0/24[V]	0		Et1/0	10.2.3.3
29	22	A::4:5:5/128[V]	0		Et1/0	10.2.3.3
30	21	A::4:5:0/112[V]	0		Et1/0	10.2.3.3
31	23	A::4:5:4/128[V]	0		Et1/0	10.2.3.3
32	24	A::5/128[V]	0		Et1/0	10.2.3.3
33	Pop Label	10.1.2.2/32[V]	0		aggregate/vpn1	
34	Pop Label	10.1.1.1/32[V]	0		Et0/0	10.1.2.1
35	27	10.4.5.4/32[V]	0		Et1/0	10.2.3.3
Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
36	28	10.5.5.5/32[V]	0		Et1/0	10.2.3.3

Following is sample output from the standby router:

Standby-Router# **show mpls forwarding**

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
18	Pop Label	10.3.3.3/32	0		Et1/0	10.2.3.3
19	Pop Label	10.3.4.0/24	0		Et1/0	10.2.3.3
20	17	10.4.4.4/32	0		Et1/0	10.2.3.3
21	Pop Label	10.1.2.1/32[V]	0		Et0/0	10.1.2.1
22	Pop Label	A::1:2:0/112[V]	0		aggregate/vpn1	
23	Pop Label	A::1:2:1/128[V]	0		Et0/0	A::1:2:1
24	Pop Label	10.1.2.0/24[V]	0		aggregate/vpn1	
25	Pop Label	A::1:2:2/128[V]	0		aggregate/vpn1	
26	18	A::1/128[V]	0		Et0/0	
FE80::A8BB:CCFF:FE03:2101						
27	26	10.4.5.5/32[V]	0		Et1/0	10.2.3.3
28	25	10.4.5.0/24[V]	0		Et1/0	10.2.3.3
29	22	A::4:5:5/128[V]	0		Et1/0	10.2.3.3
30	21	A::4:5:0/112[V]	0		Et1/0	10.2.3.3
31	23	A::4:5:4/128[V]	0		Et1/0	10.2.3.3
32	24	A::5/128[V]	0		Et1/0	10.2.3.3
33	Pop Label	10.1.2.2/32[V]	0		aggregate/vpn1	
34	Pop Label	10.1.1.1/32[V]	0		Et0/0	10.1.2.1
35	27	10.4.5.4/32[V]	0		Et1/0	10.2.3.3
Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Switched	Label	Outgoing interface	Next Hop
36	28	10.5.5.5/32[V]	0		Et1/0	10.2.3.3

**Step 6** **show ipv6 cef vrf *vrf-name***

Use this command to show preserved forwarding entries for IPv6 and VPNv6 prefixes. This sample output is also from a PE router in a CSC configuration. Enter the command on the active and the standby router. Compare the sample output from the active router with the sample output from the standby router. Following is the output from the active router:

```
Router# show ipv6 cef vrf vrf1

::/0
  no route
::/127
  discard
A::1/128
  nexthop FE80::A8BB:CCFF:FE03:2101 Ethernet0/0 label 18
A::5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 24
A::1:2:0/112
  attached to Ethernet0/0
A::1:2:1/128
  attached to Ethernet0/0
A::1:2:2/128
  receive for Ethernet0/0
A::4:5:0/112
  nexthop 10.2.3.3 Ethernet1/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 22
FE80::/10
```

Following is sample output from the standby router:

```
Standby-Router# show ipv6 cef vrf vrf1

::/0
  no route
::/127
  discard
A::1/128
  nexthop FE80::A8BB:CCFF:FE03:2101 Ethernet0/0 label 18
A::5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 24
A::1:2:0/112
  attached to Ethernet0/0
A::1:2:1/128
  attached to Ethernet0/0
A::1:2:2/128
  receive for Ethernet0/0
A::4:5:0/112
  nexthop 10.2.3.3 Ethernet1/0 label 17 21
A::4:5:4/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 23
A::4:5:5/128
  nexthop 10.2.3.3 Ethernet1/0 label 17 22
FE80::/10
```

# Configuration Examples for Configuring NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

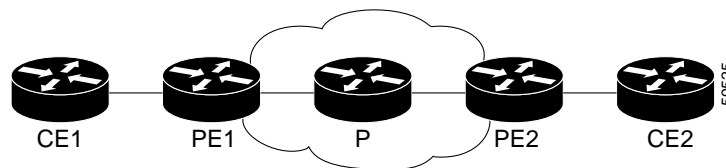
This section provides the following configuration examples for PE1 Routers.

- [Configuring NSF/SSO for a Basic 6VPE Setup: Example, page 12](#)
- [Configuring NSF/SSO for a Basic 6PE Setup: Example, page 14](#)

## Configuring NSF/SSO for a Basic 6VPE Setup: Example

This section shows the NSF/SSO configuration for a basic 6VPE setup. [Figure 1](#) show a sample basic 6VPE network configuration.

**Figure 1** Sample Basic 6VPE Network Configuration



## PE1 Configuration in a Basic 6VPE Setup

Following is a configuration example for a PE1 router (see [Figure 1](#)) in a basic 6VPE setup that includes VPNv6 and VPNv6 address families:

```

vrf definition vpn1
  rd 1:1
  route-target export 1:1
  route-target import 1:1
  !
  address-family ipv4
  exit-address-family
  !
  address-family ipv6
  exit-address-family
  !
  !
  ip cef distributed
  !
  ipv6 unicast-routing
  ipv6 cef distributed
  mpls ldp graceful-restart ! <==+ Command to configure LDP Graceful Restart
  mpls label protocol ldp
  redundancy
  mode sso
  interface Loopback0
    ip address 10.2.2.2 255.255.255.255
    ipv6 address A::2/128
  !
  interface Ethernet0/0
    vrf forwarding vpn1
    ip address 10.1.2.2 255.255.255.0
    ipv6 address A::1:2:2/112
  
```

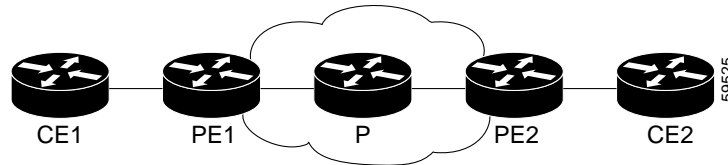
```
!interface Ethernet1/0
 ip address 10.2.3.2 255.255.255.0
 mpls label protocol ldp
 mpls ip
!router ospf 10
 log-adjacency-changes
 nsf
 network 0.0.0.0 255.255.255.255 area 0
!
router bgp 100
 no synchronization
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120      ! <=== This command,
 bgp graceful-restart stalepath-time 360    ! <=== this command, and
 bgp graceful-restart                      ! <=== this command configures NSF/SSO for a 6VPE router.
 neighbor 10.4.4.4 remote-as 100
 neighbor 10.4.4.4 update-source Loopback0
 no auto-summary
!
 address-family vpnv4
  neighbor 10.4.4.4 activate
  neighbor 10.4.4.4 send-community extended
 exit-address-family
!
 address-family vpnv6
  neighbor 10.4.4.4 activate
  neighbor 10.4.4.4 send-community extended
 exit-address-family
!
 address-family ipv4 vrf vpn1
  no synchronization
  redistribute connected
  redistribute static
  neighbor 10.1.2.1 remote-as 200
  neighbor 10.1.2.1 update-source Ethernet0/0
  neighbor 10.1.2.1 activate
 exit-address-family
!
 address-family ipv6 vrf vpn1
  redistribute connected
  redistribute static
  no synchronization
  neighbor A::1:2:1 remote-as 200
  neighbor A::1:2:1 update-source Ethernet0/0
  neighbor A::1:2:1 activate
 exit-address-family
```



## Configuring NSF/SSO for a Basic 6PE Setup: Example

This section shows the NSF/SSO configuration for a basic 6PE setup. [Figure 2](#) shows a sample basic 6PE network configuration.

**Figure 2** Sample Basic 6PE Network Configuration



### PE1 Configuration in a Basic 6PE Setup

Following is a configuration example for the PE1 router (see [Figure 2](#)) in a basic 6PE setup:

```
ip cef distributed
!
ipv6 unicast-routing
ipv6 cef distributed
mpls ldp graceful-restart ! <=== Command to configure LDP Graceful Restart
mpls label protocol ldp
redundancy
mode sso

interface Loopback0
 ip address 10.11.11.1 255.255.255.255
 ipv6 address BEEF:11::1/64
interface Ethernet0/0
 ip address 10.50.1.2 255.255.255.0
 ipv6 address 4000::72B/64
 ipv6 address 8008::72B/64
!
interface Ethernet1/0
 ip address 10.40.1.2 255.255.255.0
 mpls ip
!
router ospf
 nsf
 network 0.0.0.0 0.0.0.0 area 0
!
router bgp 100
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120 ! <=== This command,
 bgp graceful-restart stalepath-time 360 ! <=== this command, and
 bgp graceful-restart ! <=== this command configures NSF/SSO for a 6PE
router.
 neighbor 8008::72A remote-as 200
 neighbor 10.10.10.1 remote-as 100
 neighbor 10.10.10.1 update-source Loopback0
!
address-family ipv4
 no synchronization
 redistribute connected
 no neighbor 8008::72A activate
 neighbor 10.10.10.1 activate
 no auto-summary
exit-address-family
```

```

!
address-family ipv6
 redistribute connected
 no synchronization
 neighbor 8008::72A activate
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-label
 exit-address-family

```

## Additional References

The following sections provide references related to the NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE feature.

### Related Documents

Related Topic	Document Title
Information about NSF/SSO for MPLS VPN	<a href="#"><i>NSF/SSO—MPLS VPN</i></a>
Information about and configuration tasks for Cisco nonstop forwarding	<a href="#"><i>Cisco Nonstop Forwarding</i></a>
Information about and configuration tasks for MPLS VPNs	<a href="#"><i>Configuring MPLS Layer 3 VPNs</i></a>
Information about and configuration tasks for 6VPE over MPLS	<a href="#"><i>Implementing IPv6 VPN over MPLS</i></a>
Information about and configuration tasks for 6PE over MPLS	<a href="#"><i>Implementing IPv6 over MPLS</i></a>
Information about and configuration tasks for ISSU	<a href="#"><i>Cisco IOS In Service Software Upgrade Process</i></a>
Information about and configuration tasks for SSO	<a href="#"><i>Stateful Switchover</i></a>
Information about and configuration tasks for MPLS LDP NSF/SSO and Graceful Restart	<a href="#"><i>NSF/SSO-MPLS LDP and MPLS LDP Graceful Restart</i></a>

### Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

## MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFC	Title
RFC 4659	<a href="#">BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN</a>
RFC 4724	<a href="#">Graceful Restart Mechanism for BGP</a>
RFC 4781	<a href="#">Graceful Restart Mechanism for BGP with MPLS</a>
RFC 4798	<a href="#">Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)</a>

## Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

# Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

[Table 1](#) lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.2(1) or a later release appear in the table.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

[Table 1](#) lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE

Feature Name	Releases	Feature Information
ISSU—MPLS VPN 6VPE and 6PE ISSU Support	12.2(33)SRE 12.2(33)XNE	<p>This feature provides In Service Software Upgrade (ISSU) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) over Multiprotocol Label Switching (MPLS) and Cisco IOS IPv6 provider edge router (6PE) over MPLS.</p> <p>In 12.2(33)SRE, this feature was introduced on the Cisco 7600 series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li><a href="#">Elements Supporting NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE Features, page 3</a></li> <li><a href="#">ISSU Support for MPLS VPN 6vPE and 6PE, page 4</a></li> </ul> <p>This feature introduced no new or modified commands.</p>

**Table 1**      **Feature Information for NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE (continued)**

Feature Name	Releases	Feature Information
SSO—MPLS VPN 6VPE and 6PE SSO Support	12.2(33)SRE 12.2(33)XNE	<p>This feature provides stateful switchover (SSO) support for Cisco IOS Virtual Private Network (VPN) IPv6 provider edge router (6VPE) over Multiprotocol Label Switching (MPLS) and Cisco IOS IPv6 provider edge router (6PE) over MPLS.</p> <p>In 12.2(33)SRE, this feature was introduced on the Cisco 7600 series routers.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>• <a href="#">Elements Supporting NSF/SSO and ISSU—MPLS VPN 6VPE and 6PE Features, page 3</a></li> <li>• <a href="#">How BGP Graceful Restart Works for MPLS VPN 6vPE and 6PE, page 3</a></li> <li>• <a href="#">How BGP Graceful Restart Preserves Prefix Information During a Restart, page 3</a></li> <li>• <a href="#">NSF/SSO Support for MPLS VPN 6VPE and 6PE, page 4</a></li> <li>• <a href="#">BGP Graceful Restart Support for MPLS VPN Configurations, page 5</a></li> </ul> <p>This feature introduced no new or modified commands.</p>

# Glossary

**6PE router**—IPv6 provider edge (PE) router. A router running a Border Gateway Protocol (BGP)-based mechanism to interconnect IPv6 islands over a Multiprotocol Label Switching (MPLS)-enabled IPv4 cloud.

**6VPE router**—Provider edge router providing Border Gateway Protocol (BGP)-Multiprotocol Label Switching (MPLS) IPv6 Virtual Private Network (VPN) service over an IPv4-based MPLS core. It is a IPv6 VPN provider edge (PE), dual-stack router that implements 6PE concepts on the core-facing interfaces.

**BGP**—Border Gateway Protocol. An interdomain routing protocol designed for the global Internet. Exterior Border Gateway Protocols (eBGPs) communicate among different autonomous systems. Interior Border Gateway Protocols (iBGPs) communicate among routers within a single autonomous system.

**CE router**—customer edge router. A router that is part of a customer network and interfaces to a provider edge (PE) router.

**Cisco Express Forwarding**—An advanced Layer 3 IP switching technology. It optimizes network performance and scalability for all kinds of networks.

**eBGP**—external Border Gateway Protocol.

**graceful restart**—A process for helping an RP restart after a node failure has occurred.

**iBGP**—Interior Border Gateway Protocol.

**ISSU**—In Service Software Upgrade. Software upgrade without service interruption.

**LDP**—Label Distribution Protocol. A standard protocol between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets.

**MPLS**—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the routers and switches in the network where to forward the packets based on preestablished IP routing information.

**NSF**—nonstop forwarding. The ability of a router to continue to forward traffic to a router that may be recovering from a failure. Also, the ability of a router recovering from a failure to continue to correctly forward traffic sent to it by a peer.

**PE router**—provider edge router. The PE router is the entry point into the service provider network. The PE router is typically deployed on the edge of the network and is administered by the service provider. The PE router is the redistribution point between EIGRP and BGP in PE to CE networking.

**RIB**—Routing Information Base. Also called the routing table.

**SSO**—stateful switchover. SSO refers to the implementation of Cisco IOS software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. Along with NSF, SSO makes an RP failure undetectable to the network.

**VPN**—Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting traffic from one network to another. A VPN uses tunneling to encrypt all information at the IP level.

**VRF**—Virtual Private Network (VPN) routing and forwarding instance. A VRF consists of an IP routing table, a derived routing table, a set of interfaces that use the forwarding table, and a set of rules and routing information that defines a customer VPN site that is attached to a provider edge (PE) router.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks;

Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

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

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

© 2009 Cisco Systems, Inc. All rights reserved.