



MPLS Traffic Engineering Path Calculation and Setup Configuration Guide, Cisco IOS Release 15M&T

First Published: November 21, 2012

Last Modified: March 29, 2013

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 NON-INFRINGEMENT 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.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

© 2012-2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

MPLS Traffic Engineering and Enhancements 1

- Finding Feature Information 1
- Prerequisites for MPLS Traffic Engineering and Enhancements 1
- Restrictions for MPLS Traffic Engineering and Enhancements 2
- Information About MPLS Traffic Engineering and Enhancements 3
 - Introduction to MPLS Traffic Engineering and Enhancements 3
 - Benefits of MPLS Traffic Engineering 4
 - How MPLS Traffic Engineering Works 4
 - Mapping Traffic into Tunnels 5
 - Enhancement to the SPF Computation 5
 - Special Cases and Exceptions for SPF Calculations 6
 - Additional Enhancements to SPF Computation Using Configured Tunnel Metrics 7
 - Transition of an IS-IS Network to a New Technology 8
 - Extensions for the IS-IS Routing Protocol 8
 - Problems with Old and New TLVs in Theory and in Practice 9
 - First Solution for Transitioning an IS-IS Network to a New Technology 9
 - Transition Actions During the First Solution 10
 - Second Solution for Transitioning an IS-IS Network to a New Technology 10
 - Transition Actions During the Second Solution 11
 - TLV Configuration Commands 11
- How to Configure MPLS Traffic Engineering and Enhancements 12
 - Configuring a Device to Support Tunnels 12
 - Configuring an Interface to Support RSVP-Based Tunnel Signaling and IGP Flooding 13
 - Configuring IS-IS for MPLS Traffic Engineering 14
 - Configuring OSPF for MPLS Traffic Engineering 15
 - Configuring an MPLS Traffic Engineering Tunnel 16
 - DEFAULT STEPS 19
 - Configuring an MPLS Traffic Engineering Tunnel that an IGP Can Use 21

DEFAULT STEPS	21
Configuration Examples for MPLS Traffic Engineering and Enhancements	22
Configuring MPLS Traffic Engineering Using IS-IS Example	22
Router 1--MPLS Traffic Engineering Configuration	23
Router 1--IS-IS Configuration	23
Configuring MPLS Traffic Engineering Using OSPF Example	23
Router 1--MPLS Traffic Engineering Configuration	23
Router 1--OSPF Configuration	23
Configuring an MPLS Traffic Engineering Tunnel Example	24
Router 1--Dynamic Path Tunnel Configuration	24
Router 1--Dynamic Path Tunnel Verification	24
Router 1--Explicit Path Configuration	24
Router 1--Explicit Path Tunnel Configuration	24
Router 1--Explicit Path Tunnel Verification	25
Configuring Enhanced SPF Routing over a Tunnel Example	25
Router 1--IGP Enhanced SPF Consideration Configuration	25
Router 1--Route and Traffic Verification	25
Additional References	25
Feature Information for MPLS Traffic Engineering and Enhancements	27
Glossary	29

CHAPTER 2
MPLS Traffic Engineering Configurable Path Calculation Metric for Tunnels 31

Finding Feature Information	31
Feature Overview	32
Benefits	32
Restrictions	32
Related Features and Technologies	32
Prerequisites	33
Configuration Tasks	33
Configuring a Platform to Support Traffic Engineering Tunnels	33
Configuring IS-IS for MPLS Traffic Engineering	33
Configuring OSPF for MPLS Traffic Engineering	34
Configuring Traffic Engineering Link Metrics	36
Configuring an MPLS Traffic Engineering Tunnel	36
Configuring the Metric Type for Tunnel Path Calculation	37

Verifying the Configuration	38
Configuration Examples	38
Additional References	40
Feature Information for MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels	42

CHAPTER 3**MPLS Traffic Engineering Scalability Enhancements 45**

Finding Feature Information	45
Prerequisites for MPLS Traffic Engineering Scalability Enhancements	46
Restrictions for MPLS Traffic Engineering Scalability Enhancements	46
Information About MPLS Traffic Engineering Scalability Enhancements	46
Scalability Enhancements for Traffic Engineering Tunnels	46
RSVP Rate Limiting	46
Improved Recovery Response for Signaling and Management of MPLS Traffic Engineering Tunnels	47
IS-IS and MPLS Traffic Engineering Topology Database Interactions	47
Improved Counter Capabilities for MPLS TE Tunnels Events and RSVP Signaling	47
Benefits of MPLS Traffic Engineering Scalability Enhancements	48
How to Configure MPLS Traffic Engineering Scalability Enhancements	48
Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements	48
Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels	50
Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database	51
Monitoring and Maintaining MPLS TE Scalability Enhancements	52
Configuration Examples for MPLS Traffic Engineering Scalability Enhancements	55
Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements Examples	55
Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels Example	56
Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database Example	56
Additional References	56
Feature Information for MPLS Traffic Engineering Scalability Enhancements	58
Glossary	59

CHAPTER 4**MPLS Traffic Engineering--LSP Attributes 61**

Finding Feature Information	61
-----------------------------	----

Prerequisites for MPLS Traffic Engineering--LSP Attributes	62
Restrictions for MPLS Traffic Engineering--LSP Attributes	62
Information About MPLS Traffic Engineering--LSP Attributes	62
MPLS Traffic Engineering--LSP Attributes Benefits	62
Traffic Engineering Bandwidth and Bandwidth Pools	62
LSP Attribute Lists Usage and Management	63
Tunnel Attributes and LSP Attributes	63
LSP Attributes and the LSP Attribute List	63
LSP Attribute Lists Management	63
Autobandwidth and Path Option for Bandwidth Override	64
Path Option Selection for MPLS TE Tunnel LSPs	64
Constraint-Based Routing and Path Option Selection	64
Tunnel Reoptimization and Path Option Selection	65
Path Option Selection with Bandwidth Override	65
How to Configure MPLS Traffic Engineering--LSP Attributes	66
Configuring MPLS Traffic Engineering LSP Attribute Lists	66
Configuring an LSP Attribute List	66
Adding Attributes to an LSP Attribute List	69
Removing an Attribute from an LSP Attribute List	71
Modifying an Attribute in an LSP Attribute List	72
Deleting an LSP Attribute List	74
Verifying Attributes Within an LSP Attribute List	76
Verifying All LSP Attribute Lists	77
Associating an LSP Attribute List with a Path Option for an MPLS TE Tunnel	78
Modifying a Path Option to Use a Different LSP Attribute List	81
Removing a Path Option for an LSP for an MPLS TE Tunnel	83
Verifying that LSP Is Signaled Using the Correct Attributes	85
Configuring a Path Option for Bandwidth Override	86
Configuring Fallback Bandwidth Path Options for TE Tunnels	86
Modifying the Bandwidth on a Path Option for Bandwidth Override	88
Removing a Path Option for Bandwidth Override	90
Verifying that LSP Is Signaled Using the Correct Bandwidth	92
Troubleshooting Tips	93
Configuration Examples for MPLS Traffic Engineering--LSP Attributes	94
Configuring LSP Attribute List Examples	94

Configuring an LSP Attribute List Example	94
Adding Attributes to an LSP Attribute List Example	94
Removing an Attribute from an LSP Attribute List Example	94
Modifying an Attribute in an LSP Attribute List Example	95
Deleting an LSP Attribute List Example	95
Associating an LSP Attribute List with a Path Option for a TE Tunnel Example	95
Modifying a Path Option to Use a Different LSP Attribute List Example	96
Removing a Path Option for an LSP for an MPLS TE Tunnel Example	96
Configuring a Path Option for Bandwidth Override Examples	96
Path Option for Bandwidth Override and LSP Attribute List and Configuration Command Examples	97
Configuring Fallback Bandwidth Path Options for TE Tunnels Example	97
Modifying the Bandwidth on a Path Option for Bandwidth Override Example	98
Removing a Path Option for Bandwidth Override Example	98
Additional References	98
Feature Information for MPLS Traffic Engineering LSP Attributes	100
Glossary	101

CHAPTER 5**MPLS Traffic Engineering AutoTunnel Mesh Groups 103**

Finding Feature Information	103
Prerequisites for MPLS Traffic Engineering--AutoTunnel Mesh Groups	104
Restrictions for MPLS Traffic Engineering--AutoTunnel Mesh Groups	104
Information About MPLS Traffic Engineering--AutoTunnel Mesh Groups	104
AutoTunnel Mesh Groups Description and Benefits	104
Access Lists for Mesh Tunnel Interfaces	105
AutoTunnel Template Interfaces	105
OSPF Flooding of Mesh Group Information	105
How to Configure MPLS Traffic Engineering--AutoTunnel Mesh Groups	106
Configuring a Mesh of TE Tunnel LSPs	106
Enabling Autotunnel Mesh Groups Globally	106
Creating an Access List Using a Name	107
Creating an Autotunnel Template Interface	108
Specifying the Range of Mesh Tunnel Interface Numbers	111
Displaying Configuration Information About Tunnels	112
Monitoring the Autotunnel Mesh Network	113

Troubleshooting Tips	114
Configuring IGP Flooding for Autotunnel Mesh Groups	115
Configuration Examples for MPLS Traffic Engineering--Autotunnel Mesh Groups	116
Examples: Configuring a Mesh of TE Tunnel LSPs	116
Example: Enabling Autotunnel Mesh Groups Globally	117
Example: Creating an Access List Using a Name	117
Example: Creating an AutoTunnel Template Interface	117
Example: Specifying the Range of Mesh Tunnel Interface Numbers	117
Example: Configuring IGP Flooding for Autotunnel Mesh Groups	118
Additional References	118
Feature Information for MPLS Traffic Engineering--Autotunnel Mesh Groups	118
Glossary	120

CHAPTER 6**MPLS Traffic Engineering Verbatim Path Support 123**

Finding Feature Information	123
Prerequisites for MPLS Traffic Engineering--Verbatim Path Support	124
Restrictions for MPLS Traffic Engineering--Verbatim Path Support	124
Information About MPLS Traffic Engineering--Verbatim Path Support	124
How to Configure MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels	125
Configuring MPLS Traffic Engineering--Verbatim Path Support	125
Verifying Verbatim LSPs for MPLS TE Tunnels	128
Configuration Examples for MPLS Traffic Engineering Verbatim Path Support	128
Configuring MPLS Traffic Engineering: Verbatim Path Support	128
Additional References	129
Feature Information for MPLS Traffic Engineering Verbatim Path Support	130
Glossary	131

CHAPTER 7**MPLS Traffic Engineering RSVP Hello State Timer 133**

Finding Feature Information	133
Prerequisites for MPLS Traffic Engineering--RSVP Hello State Timer	134
Restrictions for MPLS Traffic Engineering--RSVP Hello State Timer	134
Information About MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels	134
Hellos for State Timeout	134

Nonfast-Reroutable TE LSP	134
Hello Instance	135
Fast-Reroutable TE LSP with Backup Tunnel	135
Fast-Reroutable TE LSP Without Backup Tunnel	136
How to Configure MPLS Traffic Engineering--RSVP Hello State Timer	137
Enabling the Hello State Timer Globally	137
Enabling the Hello State Timer on an Interface	138
Setting a DSCP Value on an Interface	139
Setting a Hello Request Interval on an Interface	140
Setting the Number of Hello Messages that can be Missed on an Interface	141
Verifying Hello for State Timer Configuration	142
Configuration Examples for MPLS Traffic Engineering--RSVP Hello State Timer	143
Example	143
Additional References	143
Command Reference	145
Feature Information for MPLS Traffic Engineering--RSVP Hello State Timer	145
Glossary	146

CHAPTER 8

MPLS Traffic Engineering Forwarding Adjacency	149
Finding Feature Information	149
Prerequisites for MPLS Traffic Engineering Forwarding Adjacency	150
Restrictions for MPLS Traffic Engineering Forwarding Adjacency	150
Information About MPLS Traffic Engineering Forwarding Adjacency	150
MPLS Traffic Engineering Forwarding Adjacency Functionality	150
MPLS Traffic Engineering Forwarding Adjacency Benefits	151
How to Configure MPLS Traffic Engineering Forwarding Adjacency	151
Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency	151
Configuring MPLS TE Forwarding Adjacency on Tunnels	152
Verifying MPLS TE Forwarding Adjacency	154
Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency	155
Example MPLS TE Forwarding Adjacency	155
Usage Tips	156
Additional References	157
Glossary	158
Feature Information for MPLS Traffic Engineering Forwarding Adjacency	159

CHAPTER 9**MPLS Traffic Engineering Interarea Tunnels 161**

- Finding Feature Information **161**
- Prerequisites for MPLS Traffic Engineering Interarea Tunnels **162**
- Restrictions for MPLS Traffic Engineering Interarea Tunnels **162**
- Information About MPLS Traffic Engineering Interarea Tunnels **162**
 - Interarea Tunnels Functionality **162**
 - Autoroute Destination Functionality **164**
 - CBTS Interaction with Autoroute Destination **164**
 - Manually Configured Static Routes Interaction with Autoroute Destination **164**
 - Autoroute Announce Interaction with Autoroute Destination **164**
 - Forwarding Adjacency Interaction with Autoroute Destination **164**
 - MPLS Traffic Engineering Interarea Tunnels Benefits **164**
- How to Configure MPLS Traffic Engineering Interarea Tunnels **165**
 - Configuring OSPF for Interarea Tunnels **165**
 - Configuring OSPF for ABR Routers **165**
 - Configuring OSPF for Non-ABR Routers **167**
 - Configuring IS-IS for Interarea Tunnels **168**
 - Configuring IS-IS for Backbone Routers **168**
 - Configuring IS-IS for Nonbackbone Routers **170**
 - Configuring IS-IS for Interfaces **172**
 - Configuring MPLS and RSVP to Support Traffic Engineering **174**
 - Configuring an MPLS Traffic Engineering Interarea Tunnel **175**
 - Configuring an MPLS Traffic Engineering Interarea Tunnel to Use Explicit Paths **175**
 - Configuring Explicit Paths **177**
 - Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination **178**
- Configuration Examples for MPLS Traffic Engineering Interarea Tunnels **180**
 - Configuring OSPF for Interarea Tunnels Example **180**
 - Configuring IS-IS for Interarea Tunnels Example **182**
 - Configuring MPLS and RSVP to Support Traffic Engineering Example **183**
 - Configuring an MPLS Traffic Engineering Interarea Tunnel Example **184**
 - Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination Example **184**
- Additional References **185**
- Feature Information for MPLS Traffic Engineering Interarea Tunnels **186**

Glossary 187

CHAPTER 10

MPLS Traffic Engineering Class-based Tunnel Selection 191

- Finding Feature Information 192
- Prerequisites for MPLS Traffic Engineering Class-based Tunnel Selection 192
- Restrictions for MPLS Traffic Engineering Class-based Tunnel Selection 192
- Information About MPLS Traffic Engineering Class-based Tunnel Selection 192
 - Incoming Traffic Supported by MPLS TE Class-based Tunnel Selection 192
 - CoS Attributes for MPLS TE Class-based Tunnel Selection 193
 - Routing Protocols and MPLS TE Class-based Tunnel Selection 193
 - Tunnel Selection with MPLS TE Class-based Tunnel Selection 193
 - EXP Mapping Configuration 193
 - Tunnel Selection for EXP Values 194
 - Tunnel Failure Handling 197
 - Misordering of Packets 199
 - Fast Reroute and MPLS TE Class-based Tunnel Selection 199
 - DS-TE Tunnels and MPLS TE Class-based Tunnel Selection 200
 - Reoptimization and MPLS TE Class-based Tunnel Selection 200
 - Interarea and Inter-AS and MPLS TE Class-based Tunnel Selection 200
 - ATM PVCs and MPLS TE Class-based Tunnel Selection 200
- How to Configure MPLS Traffic Engineering Class-based Tunnel Selection 200
 - Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend 201
 - Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel 203
 - Making the MPLS TE or DS-TE Tunnels Visible for Routing 204
 - Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP 206
 - Configuring a Master Tunnel 208
- Configuration Examples for MPLS Traffic Engineering Class-based Tunnel Selection 210
 - Example: Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend 210
 - Example: Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel 210
 - Making the MPLS TE or DS-TE Tunnels Visible for Routing Example 210
 - Example: Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP 211
 - Example: Configuring a Master Tunnel 216

Additional References	217
Feature Information for MPLS Traffic Engineering Class-based Tunnel Selection	217
Glossary	218

CHAPTER 11**MPLS Traffic Engineering Automatic Bandwidth Adjustment for TE Tunnels 221**

Finding Feature Information	221
Prerequisites for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels	222
Restrictions for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels	222
Information About MPLS TE Automatic Bandwidth Adjustment for TE Tunnels	222
MPLS TE Automatic Bandwidth Adjustment for TE Tunnels Overview	222
MPLS TE Automatic Bandwidth Adjustment for TE Tunnels Benefits	223
How to Configure MPLS TE Automatic Bandwidth Adjustment for TE Tunnels	223
Configuring a Device to Support Traffic Engineering Tunnels	223
Configuring IS-IS or OSPF for MPLS Traffic Engineering	224
Configuring IS-IS for MPLS Traffic Engineering	224
Configuring OSPF for MPLS Traffic Engineering	226
Configuring Bandwidth on Each Link That a Tunnel Crosses	227
Configuring an MPLS Traffic Engineering Tunnel	228
Troubleshooting Tips	231
Enabling Automatic Bandwidth Adjustment on a Platform	231
Enabling Automatic Bandwidth Adjustment for a Tunnel	232
Configuring the Interval for Computing the Tunnel Average Output Rate	234
Verifying Automatic Bandwidth Configuration	235
Configuration Examples for MPLS TE Automatic Bandwidth Adjustments for TE Tunnels	237
Example: Configuring MPLS Traffic Engineering Automatic Bandwidth	238
Example: Tunnel Configuration for Automatic Bandwidth	238
Additional References	238
Feature Information for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels	240

CHAPTER 12**MPLS Traffic Engineering Tunnel Source 241**

Finding Feature Information	241
Prerequisites for MPLS Traffic Engineering Tunnel Source	241
Restrictions for MPLS Traffic Engineering Tunnel Source	242
Information About MPLS Traffic Engineering Tunnel Source	242

MPLS Traffic Engineering Tunnel Source Usage Guidelines	242
How to Configure MPLS Traffic Engineering Tunnel Source	242
Configuring MPLS Traffic Engineering Tunnel Source	242
Configuration Examples for MPLS Traffic Engineering Tunnel Source	245
MPLS Traffic Engineering Tunnel Source Example	245
Additional References	246
Feature Information for MPLS Traffic Engineering Tunnel Source	247



CHAPTER

1

MPLS Traffic Engineering and Enhancements

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

- [Finding Feature Information, page 1](#)
- [Prerequisites for MPLS Traffic Engineering and Enhancements, page 1](#)
- [Restrictions for MPLS Traffic Engineering and Enhancements, page 2](#)
- [Information About MPLS Traffic Engineering and Enhancements, page 3](#)
- [How to Configure MPLS Traffic Engineering and Enhancements, page 12](#)
- [Configuration Examples for MPLS Traffic Engineering and Enhancements, page 22](#)
- [Additional References, page 25](#)
- [Feature Information for MPLS Traffic Engineering and Enhancements, page 27](#)
- [Glossary, page 29](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering and Enhancements

Your network must support the following Cisco IOS features before you enable MPLS traffic engineering:

- Multiprotocol Label Switching
- IP Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

Restrictions for MPLS Traffic Engineering and Enhancements

- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.
- MPLS traffic engineering does not support ATM MPLS-controlled subinterfaces.
- The MPLS traffic engineering feature does not support routing and signaling of LSPs over unnumbered IP links. Therefore, do not configure the feature over those links.
- When specifying an explicit path for an MPLS TE tunnel, you can specify link or node addresses of the next-hop routers in an explicit path. You can also specify a mixture of link and node addresses. However, there are some restrictions:
 - In Cisco IOS Release 12.2(33)SRD, 12.4(24)T and earlier releases, you cannot specify an explicit path that uses a link address as the first hop and then node addresses as the subsequent hops. However, you can use a node address as the first hop and link addresses as the subsequent hops.
 - In Cisco IOS Releases after Cisco IOS Release 12.2(33)SRD and 12.4(24)T, you can use a link address as the first hop and then node addresses as the subsequent hops. There are no restrictions when specifying a mixture of link and node addresses.
- When specifying an explicit path, if you specify the “forward” address (the address of the interface that forwards the traffic to the next router) as the next-hop address, the explicit path might not be used. Using the forward address allows that entry to be treated as a loose hop for path calculation. Cisco recommends that you use the “receive” address (the address of the interface that receives traffic from the sending router) as the next-hop address.

In the following example, router R3 sends traffic to router R1. The paths marked a,b and x,y between routers R1 and R2 are parallel paths.

```
R1 (a) ---- (b) R2 (c) -- (d) R3
      (x) ---- (y)
```

If you configure an explicit path from R3 to R1 using the “forward” addresses (addresses d and b), the tunnel might reroute traffic over the parallel path (x,y) instead of the explicit path. To ensure that the tunnel uses the explicit path, specify the “receive” addresses as part of the **next-address** command, as shown in the following example:

```
ip explicit-path name path1
  next-address (c)
  next-address (a)
```


Information About MPLS Traffic Engineering and Enhancements

Introduction to MPLS Traffic Engineering and Enhancements

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

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

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

MPLS traffic engineering supports the following functionality:

- Enhances standard Interior Gateway Protocols (IGPs), such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows.
- Transports traffic flows across a network using MPLS forwarding.
- Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.
- Employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS traffic engineering, the traffic flow has bandwidth requirements, media requirements, a priority that is compared to the priority of other flows, and so forth.
- Recovers from link or node failures by adapting to the new constraints presented by the changed topology.
- Transports packets using MPLS forwarding crossing a multihop label switched path (LSP).
- Uses the routing and signaling capability of LSPs across a backbone topology that
 - Understands the backbone topology and available resources
 - Accounts for link bandwidth and for the size of the traffic flow when determining routes for LSPs across the backbone
 - Has a dynamic adaptation mechanism that enables the backbone to be resilient to failures, even if several primary paths are precalculated off-line
 - Includes enhancements to the IGP (IS-IS or OSPF) shortest path first (SPF) calculations to automatically calculate what traffic should be sent over what LSPs.

Benefits of MPLS Traffic Engineering

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

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

How MPLS Traffic Engineering Works

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

Available resources are flooded by means of extensions to a link-state based IGP.

Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint-based routing). The IGP automatically routes the traffic onto these LSPs. Typically, a packet crossing the MPLS traffic engineering backbone travels on a single LSP that connects the ingress point to the egress point.

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

- IP tunnel interfaces

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

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

- MPLS traffic engineering path calculation module

This calculation module operates at the LSP head. The module determines a path to use for an LSP. The path calculation uses a link-state database containing flooded topology and resource information.

- RSVP with traffic engineering extensions

RSVP operates at each LSP hop and is used to signal and maintain LSPs based on the calculated path.

- MPLS traffic engineering link management module

This module operates at each LSP hop, does link call admission on the RSVP signaling messages, and bookkeeping of topology and resource information to be flooded.

- Link-state IGP (IS-IS or OSPF--each with traffic engineering extensions)

These IGPs are used to globally flood topology and resource information from the link management module.

- Enhancements to the SPF calculation used by the link-state IGP (IS-IS or OSPF)

The IGP automatically routes traffic onto the appropriate LSP tunnel based on tunnel destination. Static routes can also be used to direct traffic onto LSP tunnels.

- Label switching forwarding

This forwarding mechanism provides routers with a Layer 2-like ability to direct traffic across multiple hops of the LSP established by RSVP signaling.

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

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

Mapping Traffic into Tunnels

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

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

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

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

Enhancement to the SPF Computation

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

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

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

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

The router must determine the first-hop information. There are several ways to do this:

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

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

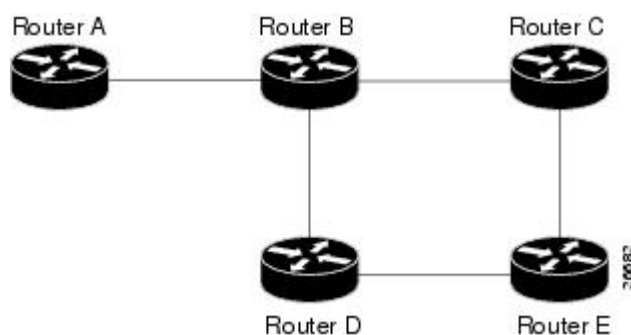
Special Cases and Exceptions for SPF Calculations

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

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

A special situation occurs in the topology shown in the figure below.

Figure 1: Sample Topology of Parallel Native Paths and Paths Over TE Tunnels



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

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

Traffic to Router E now load balances over

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

Additional Enhancements to SPF Computation Using Configured Tunnel Metrics

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

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

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

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

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

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

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

In each of the above cases, the IGP assigns metrics to routes associated with those tailend routers and their downstream routers.

The SPF computation is loop free because the traffic through the TE tunnels is basically source routed. The end result of TE tunnel metric adjustment is the control of traffic loadsharing. If there is only one way to reach

the destination through a single TE tunnel, then no matter what metric is assigned, the traffic has only one way to go.

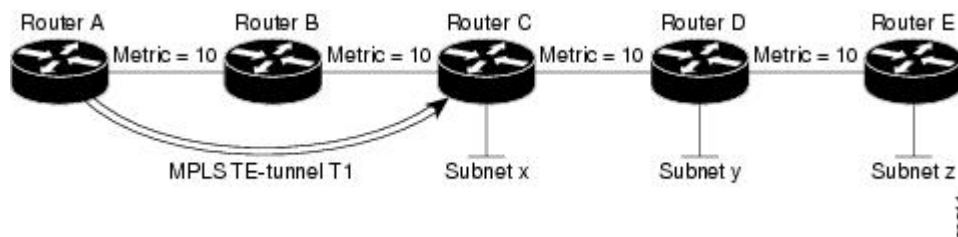
You can represent the TE tunnel metric in two different ways: (1) as an absolute (or fixed) metric or (2) as a relative (or floating) metric.

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

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

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

Figure 2: Topology That Has No Traffic Engineering Tunnel



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

Transition of an IS-IS Network to a New Technology

IS-IS, as specified in RFC 1142, includes extensions for MPLS traffic engineering and for other purposes. Running MPLS traffic engineering over IS-IS or taking advantage of these other extensions requires transitioning an IS-IS network to this new technology. This section describes these extensions and discusses two ways to migrate an existing IS-IS network from the standard ISO 10589 protocol towards the version of IS-IS specified in RFC 1142. Running MPLS traffic engineering over an existing IS-IS network requires a transition to the version of IS-IS specified in RFC 1142. However, running MPLS traffic engineering over OSPF does **not** require any similar network transition.

This section contains information about the following topics:

Extensions for the IS-IS Routing Protocol

Extensions for the IS-IS routing protocol serve the following purposes:

- Remove the 6-bit limit on link metrics.
- Allow interarea IP routes.

- Enable IS-IS to carry different kinds of information for traffic engineering. In the future, more extensions might be needed.

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

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

**Note**

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

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

Problems with Old and New TLVs in Theory and in Practice

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

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

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

Network administrators have the following problems related to TLVs:

- They need to run an IS-IS network where some routers are advertising and using the new-style TLVs and, at the same time, other routers are capable only of advertising and using old-style TLVs.
- They need to test new traffic engineering software in existing networks on a limited number of routers. They cannot upgrade all their routers in their production networks or in their test networks before they start testing.

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

The following sections describe two solutions to the network administrator's problems.

First Solution for Transitioning an IS-IS Network to a New Technology

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

There are three disadvantages to using that approach:

- Size of the LSPs--During the transition, the LSPs grow to about twice their original size. This might be a problem in networks where the LSPDB is large. An LSPDB might be large because
 - There are many routers, and thus LSPs.
 - There are many neighbors or IP prefixes per router. A router that advertises lots of information causes the LSPs to be fragmented.
- Unpredictable results--In a large network, this solution can produce unpredictable results. A large network in transition pushes the limits regarding LSP flooding and SPF scaling. During the transition
 - You can expect some extra network instability. At this time, you especially do not want to test how far you can push an implementation.
 - Traffic engineering extensions might cause LSPs to be reflooded frequently.
- Ambiguity--If a router encounters different information in the old-style TLVs and the new-style TLVs, it may not be clear what the router should do.

These problems can be largely solved easily by using

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

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

Transition Actions During the First Solution

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

- If all routers run old software, advertise and use only old-style TLVs.
- Upgrade some routers to newer software.
- Configure some routers with new software to advertise both old-style and new-style TLVs. They accept both styles of TLVs. Configure other routers (with old software) to continue advertising and using only old-style TLVs.
- Test traffic engineering in parts of your network; however, new-style TLVs cannot be used yet.
- If the whole network needs to migrate, upgrade and configure all remaining routers to advertise and accept both styles of TLVs.
- Configure all routers to advertise and accept only new-style TLVs.
- Configure metrics larger than 63.

For more information about how to perform these actions, see the TLV Configuration Commands section.

Second Solution for Transitioning an IS-IS Network to a New Technology

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

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

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

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

Transition Actions During the Second Solution

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

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

TLV Configuration Commands

Cisco IOS has a **router isis** command-line interface (CLI) command called **metric-style**. Once the router is in IS-IS configuration mode, you have the option to choose the following:

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

You can use either of the following two transition schemes when you use the **metric-style** command to configure:

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

How to Configure MPLS Traffic Engineering and Enhancements

Configuring a Device to Support Tunnels

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip cef`
4. `mpls traffic-eng tunnels`
5. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip cef Example: Router(config)# ip cef	Enables standard Cisco Express Forwarding operation.
Step 4	mpls traffic-eng tunnels Example: Router(config)# mpls traffic-eng tunnels	Enables the MPLS traffic engineering tunnel feature on a device.
Step 5	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

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



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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / subslot / port* [*.subinterface-number*]
4. **mpls traffic-eng tunnels**
5. **ip rsvp bandwidth** *bandwidth*
6. **exit**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type slot / subslot / port</i> [<i>.subinterface-number</i>] Example: Router(config)# interface serial 1/0/0	Configures an interface type and enters interface configuration mode.
Step 4	mpls traffic-eng tunnels Example: Router(config-if)# mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnels on an interface.

	Command or Action	Purpose
Step 5	ip rsvp bandwidth <i>bandwidth</i> Example: Router(config-if)# ip rsvp bandwidth 1000	Enables RSVP for IP on an interface and specifies the amount of bandwidth that will be reserved.
Step 6	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 7	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the following steps.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

SUMMARY STEPS

1. Router(config)# **router isis**
2. Router(config-router)# **mpls traffic-eng level-1**
3. Router(config-router)# **mpls traffic-eng level-2**
4. Router(config-router)# **mpls traffic-eng router-id loopback 0**
5. Router(config-router)# **metric-style wide**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# router isis	Enables IS-IS routing and specifies an IS-IS process for IP. The router is placed in configuration mode.

	Command or Action	Purpose
Step 2	Router(config-router)# mpls traffic-eng level-1	Turns on MPLS traffic engineering for IS-IS level 1.
Step 3	Router(config-router)# mpls traffic-eng level-2	Turns on MPLS traffic engineering for IS-IS level 2.
Step 4	Router(config-router)# mpls traffic-eng router-id loopback 0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.
Step 5	Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style type, length, value objects (TLVs).

Configuring OSPF for MPLS Traffic Engineering

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	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Router(config)# router ospf 200	Configures an OSPF routing process for IP and enters router configuration mode. • The value for the <i>process-id</i> argument is an internally used identification parameter for an OSPF routing process. It

	Command or Action	Purpose
		is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process.
Step 4	mpls traffic-eng area <i>number</i> Example: <pre>Router(config-router)# mpls traffic-eng area 0</pre>	Turns on MPLS TE for the indicated OSPF area.
Step 5	mpls traffic-eng router-id <i>loopback0</i> Example: <pre>Router(config-router)# mpls traffic-eng router-id loopback0</pre>	Specifies that the TE router identifier for the node is the IP address associated with interface loopback0.
Step 6	exit Example: <pre>Router(config-router)# exit</pre>	Exits to global configuration mode.
Step 7	exit Example: <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.

Configuring an MPLS Traffic Engineering Tunnel

This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
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* {dynamic | explicit {name *path-name* | identifier *path-number*}}** [lockdown]
9. **exit**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface Tunnel0	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> • The <i>number</i> argument is the number of the tunnel.
Step 4	ip unnumbered <i>type number</i> Example: Router(config-if)# ip unnumbered loopback0	Enables IP processing on an interface without assigning an explicit IP address to the interface. <ul style="list-style-type: none"> • 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. • An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.
Step 5	tunnel destination <i>ip-address</i>	Specifies the destination for a tunnel interface.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-if)# tunnel destination 192.168.4.4</pre>	<ul style="list-style-type: none"> The <i>ip-address</i> argument must be the MPLS traffic engineering router ID of the destination device.
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 7	<p>tunnel mpls traffic-eng bandwidth <i>bandwidth</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 250</pre>	<p>Configures the bandwidth for the MPLS traffic engineering tunnel.</p> <ul style="list-style-type: none"> The <i>bandwidth</i> argument is a number in kilobits per second that is set aside for the MPLS traffic engineering tunnel. Range is from 1 to 4294967295. <p>Note If automatic bandwidth is configured for the tunnel, use the tunnel mpls traffic-eng bandwidth command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism.</p>
Step 8	<p>tunnel mpls traffic-eng path-option <i>number</i> {dynamic explicit {name <i>path-name</i> identifier <i>path-number</i>}} [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit identifier 321</pre>	<p>Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.</p> <ul style="list-style-type: none"> The <i>number</i> argument is the preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000. The dynamic keyword indicates that the path of the label switched path (LSP) is dynamically calculated. The explicit keyword indicates that the path of the LSP is an IP explicit path. The name <i>path-name</i> keyword and argument are the path name of the IP explicit path that the tunnel uses with this option. The identifier <i>path-number</i> keyword and argument pair names the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535. The lockdown keyword specifies that The LSP cannot be reoptimized. <p>Note A dynamic path is used if an explicit path is currently unavailable.</p>
Step 9	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 10	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

DEFAULT STEPS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
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* {dynamic | explicit {name *path-name*} | identifier *path-number*} [lockdown]
9. **exit**
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel10	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	ip unnumbered <i>type number</i> Example: Router(config-if)# ip unnumbered loopback 0	Gives the tunnel interface an IP address. <ul style="list-style-type: none"> • An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.
Step 5	tunnel destination <i>ip-address</i> Example: Router(config-if)# tunnel destination 10.20.1.1	Specifies the destination for a tunnel. <ul style="list-style-type: none"> • The <i>ip-address</i> keyword is the IP address of the host destination expressed in dotted decimal notation.
Step 6	tunnel mode mpls traffic-eng Example: Router(config-if)# tunnel mode mpls traffic-eng	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 7	tunnel mpls traffic-eng bandwidth <i>bandwidth</i> Example: Router(config-if)# tunnel mpls traffic-eng bandwidth 1000	Configures the bandwidth for the MPLS traffic engineering tunnel.
Step 8	tunnel mpls traffic-eng path-option <i>number</i> {dynamic explicit {name <i>path-name</i> } identifier <i>path-number</i> } [lockdown] Example: Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit identifier 1	Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database. <ul style="list-style-type: none"> • A dynamic path is used if an explicit path is currently unavailable.
Step 9	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 10	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuring an MPLS Traffic Engineering Tunnel that an IGP Can Use

This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

DEFAULT STEPS

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **tunnel mpls traffic-eng autoroute announce**
5. **exit**
6. **exit**

DETAILED STEPS

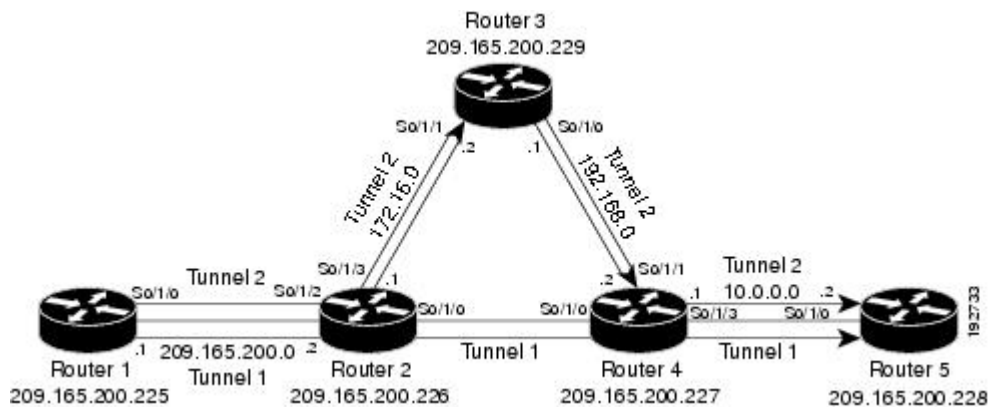
	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel1	Configures an interface type and enters interface configuration mode.
Step 4	tunnel mpls traffic-eng autoroute announce Example: Router(config-if)# tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel in its enhanced SPF calculation.
Step 5	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuration Examples for MPLS Traffic Engineering and Enhancements

The figure below illustrates a sample MPLS topology. This example specifies point-to-point outgoing interfaces. The next sections contain sample configuration commands you enter to implement MPLS traffic engineering and the basic tunnel configuration shown in Figure 3.

Figure 3: Sample MPLS Traffic Engineering Tunnel Configuration



Configuring MPLS Traffic Engineering Using IS-IS Example

This example lists the commands you enter to configure MPLS traffic engineering with IS-IS routing enabled (see the figure above).



Note

You must enter the following commands on every router in the traffic-engineered portion of your network.

Router 1--MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 10.0.0.0 255.255.255.254
ip router isis
interface s1/0/0
ip address 209.165.200.1 255.255.0.0
ip router isis
mpls traffic-eng tunnels
ip rsvp bandwidth 1000
```

Router 1--IS-IS Configuration

To enable IS-IS routing, enter the following commands:

```
router isis
network 47.0000.0011.0011.00
is-type level-1
metric-style wide
mpls traffic-eng router-id loopback0
mpls traffic-eng level-1
```

Configuring MPLS Traffic Engineering Using OSPF Example

This example lists the commands you enter to configure MPLS traffic engineering with OSPF routing enabled (see the figure above).

**Note**

You must enter the following commands on every router in the traffic-engineered portion of your network.

Router 1--MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 209.165.200.225 255.255.255.255
interface s1/0/0
ip address 209.165.200.1 255.255.0.0
mpls traffic-eng tunnels
  ip rsvp bandwidth 1000
```

Router 1--OSPF Configuration

To enable OSPF, enter the following commands:

```
router ospf 0
network 209.165.200.0.0.0.255.255 area 0
```

```
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

Configuring an MPLS Traffic Engineering Tunnel Example

This example shows you how to configure a dynamic path tunnel and an explicit path in the tunnel. Before you configure MPLS traffic engineering tunnels, you must enter the appropriate global and interface commands on the specified router (in this case, Router 1).

Router 1--Dynamic Path Tunnel Configuration

In this section, a tunnel is configured to use a dynamic path.

```
interface tunnel1
 ip unnumbered loopback 0
 tunnel destination 209.165.200.228
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 dynamic
```

Router 1--Dynamic Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up.

```
show mpls traffic-eng tunnels
show ip interface tunnel1
```

Router 1--Explicit Path Configuration

In this section, an explicit path is configured.

```
ip explicit-path identifier 1
 next-address 209.165.200.1
 next-address 172.16.0.1
 next-address 192.168.0.1
 next-address 10.0.0.1
```

Router 1--Explicit Path Tunnel Configuration

In this section, a tunnel is configured to use an explicit path.

```
interface tunnel2
 ip unnumbered loopback 0
 tunnel destination 209.165.200.228
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 explicit identifier 1
```

Router 1--Explicit Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up.

```
show mpls traffic-eng tunnels
show ip interface tunnel2
```

Configuring Enhanced SPF Routing over a Tunnel Example

This section includes the commands that cause the tunnel to be considered by the IGP's enhanced SPF calculation, which installs routes over the tunnel for appropriate network prefixes.

Router 1--IGP Enhanced SPF Consideration Configuration

In this section, you specify that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.

```
interface tunnel1
 tunnel mpls traffic-eng autoroute announce
```

Router 1--Route and Traffic Verification

This section includes the commands you use to verify that the tunnel is up and that the traffic is routed through the tunnel.

```
show traffic-eng tunnels tunnel1 brief
show ip route 209.165.200.228
show mpls traffic-eng autoroute
ping 209.165.200.228
show interface tunnel1 accounting
show interface s1/0/0 accounting
```

Additional References

The following sections provide references related to the MPLS Traffic Engineering and Enhancements feature.

Related Documents

Related Topic	Document Title
IS-IS commands	<i>Cisco IOS IP Routing Protocols Command Reference</i>
OSPF command	<i>Cisco IOS IP Routing Protocols Command Reference</i>
MPLS TE commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>
RSVP commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i>

Standards

Standard	Title
None	--

MIBs

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

RFCs

RFC	Title
1142	<i>IS-IS</i>
1195	<i>Use of OSI IS-IS for Routing in TCP/IP and Dual Environments</i>
2205	<i>Resource ReSerVation Protocol (RSVP)</i>
2328	<i>OSPF Version 2</i>
2370	<i>The OSPF Opaque LSA Option</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>http://www.cisco.com/techsupport</p>

Feature Information for MPLS Traffic Engineering and Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1: Feature Information for MPLS Traffic Engineering and Enhancements

Feature Name	Releases	Feature Information
MPLS Traffic Engineering and Enhancements	12.0(6)T 12.0(5)S 12.1(2)E 12.2(28)SB2 12.2(46)SE	<p>Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what previously could be achieved only by overlaying a Layer 3 network on a Layer 2 network.</p> <p>This feature was introduced in Cisco IOS Release 12.0(6)T.</p> <p>This feature was integrated into Cisco IOS Release 12.0(5)S.</p> <p>This feature was integrated into Cisco IOS Release 12.1(2)E.</p> <p>This feature was integrated into Cisco IOS Release 12.2(28)SB2.</p> <p>This feature was integrated into Cisco IOS Release 12.2(46)SE.</p>
		<p>The following commands were introduced or modified:ip explicit-path, metric-style narrow, metric-style transition, metric-style wide, mpls traffic-eng, mpls traffic-eng area, mpls traffic-eng router-id, mpls traffic-eng tunnels (configuration), mpls traffic-eng tunnels (interface), show mpls traffic-eng autoroute, show mpls traffic-eng tunnels, tunnel mode mpls traffic-eng, tunnel mode mpls traffic-eng autoroute announce, tunnel mpls traffic-eng bandwidth, tunnel mpls traffic-eng path-option, tunnel mpls traffic-eng priority.</p>

Glossary

affinity --An MPLS traffic engineering tunnel's requirements on the attributes of the links it will cross. The tunnel's affinity bits and affinity mask bits must match the attribute bits 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. Tunnels that are harder to route are expected to have a higher priority and to be able to preempt tunnels that are easier to route. The assumption is that lower-priority tunnels will be able to find another path.

constraint-based routing --Procedures and protocols that determine a route across a backbone take 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 is carried across one or more LSP tunnels running from the entry POP to the exit POP.

headend --The upstream, transmit end of a tunnel.

IGP --Interior Gateway Protocol. The Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include IGRP, OSPF, and RIP.

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 that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

label switched path (LSP) --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.

label switched path (LSP) tunnel --A configured connection between two routers, in which label switching is used to carry the packets.

label switching router (LSR) --A Layer 3 router that forwards packets based on the value of a label encapsulated in the packets.

LCAC --Link-level (per hop) call admission control.

LSA --Link-state advertisement. Flooded packet used by OSPF that contains information about neighbors and path costs. In IS-IS, receiving routers use LSAs to maintain their routing tables.

LSP--See label switched path.

OSPF protocol --Open Shortest Path First. A link state routing protocol used for routing IP.

reoptimization--Reevaluation of the most suitable path for a tunnel to use, given the specified constraints.

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

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.



MPLS Traffic Engineering Configurable Path Calculation Metric for Tunnels

The MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels feature enables the user to control the metric used in path calculation for traffic engineering (TE) tunnels on a per-tunnel basis. Certain tunnels are used to carry voice traffic, which requires low delay, and other tunnels are used to carry data. A TE link metric can be used to represent link delay and configure tunnels that carry voice traffic for path calculation and configure tunnels that carry data to use the Interior Gateway Protocol (IGP) metric for path calculation.

- [Finding Feature Information, page 31](#)
- [Feature Overview, page 32](#)
- [Prerequisites, page 33](#)
- [Configuration Tasks, page 33](#)
- [Configuration Examples, page 38](#)
- [Additional References, page 40](#)
- [Feature Information for MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels, page 42](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Feature Overview

When Multiprotocol Label Switching (MPLS) TE is configured in a network, the Interior Gateway Protocol (IGP) floods two metrics for every link: the normal IGP (Open Shortest Path First (OSPF) or (Intermediate System-to-Intermediate System (IS-IS)) link metric and a TE link metric. The IGP uses the IGP link metric in the normal way to compute routes for destination networks. In releases previous to Cisco IOS Release 12.2(18)ST, MPLS TE used the TE link metric to calculate and verify paths for TE tunnels. When the traffic engineering metric was not explicitly configured, the traffic engineering metric was the IGP metric.

The enhancement as of release Cisco IOS Release 12.2(18)ST allows you to specify that the path calculation for a given tunnel be based on either of the following:

- IGP link metrics.
- TE link metrics, which you can configure so that they represent the needs of a particular application. For example, the TE link metrics can be configured to represent link transmission delay.

Benefits

When TE tunnels are used to carry two types of traffic, the Configurable Path Calculation Metric for Tunnels enhancement allows you to tailor tunnel path selection to the requirements of each type of traffic.

For example, suppose certain tunnels are to carry voice traffic (which requires low delay) and other tunnels are to carry data. In this situation, you can use the TE link metric to represent link delay and do the following:

- Configure tunnels that carry voice to use the TE link metric set to represent link delay for path calculation.
- Configure tunnels that carry data to use the IGP metric for path calculation.

Restrictions

- Unless explicitly configured, the TE link metric for a given link is the IGP link metric. When the TE link metric is used to represent a link property that is different from cost/distance, you must configure every network link that can be used for TE tunnels with a TE link metric that represents that property by using the **mpls traffic-eng administrative-weight** command. Failure to do so might cause tunnels to use unexpected paths.
- You cannot configure MPLS Traffic Engineering over the logical GRE tunnel interface.
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

Related Features and Technologies

The configurable path calculation metric feature is related to MPLS TE.

Prerequisites

Before you configure tunnel path calculation metrics, your network must support the following Cisco IOS features:

- MPLS traffic engineering tunnels
- IP Cisco Express Forwarding
- OSPF or IS-IS

Configuration Tasks

See the following sections for configuration tasks for the configurable path calculation metric feature.

Configuring a Platform to Support Traffic Engineering Tunnels

To configure a platform to support traffic engineering tunnels, perform the following steps in global configuration mode:

SUMMARY STEPS

1. Router(config)# **ip cef**
2. Router(config)# **mpls traffic-eng tunnels**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# ip cef	Enables standard Cisco Express Forwarding operation.
Step 2	Router(config)# mpls traffic-eng tunnels	Enables the MPLS traffic engineering tunnel feature on a device.

Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the following steps.



Note

MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

SUMMARY STEPS

1. Router(config)# **router isis**
2. Router(config-router)# **mpls traffic-eng level-1**
3. Router(config-router)# **mpls traffic-eng level-2**
4. Router(config-router)# **mpls traffic-eng router-id loopback 0**
5. Router(config-router)# **metric-style wide**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# router isis	Enables IS-IS routing and specifies an IS-IS process for IP. The router is placed in configuration mode.
Step 2	Router(config-router)# mpls traffic-eng level-1	Turns on MPLS traffic engineering for IS-IS level 1.
Step 3	Router(config-router)# mpls traffic-eng level-2	Turns on MPLS traffic engineering for IS-IS level 2.
Step 4	Router(config-router)# mpls traffic-eng router-id loopback 0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.
Step 5	Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style type, length, value objects (TLVs).

Configuring OSPF for MPLS Traffic Engineering**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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>router ospf <i>process-id</i></p> <p>Example:</p> <pre>Router(config)# router ospf 200</pre>	<p>Configures an OSPF routing process for IP and enters router configuration mode.</p> <ul style="list-style-type: none"> 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.
Step 4	<p>mpls traffic-eng area <i>number</i></p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng area 0</pre>	Turns on MPLS TE for the indicated OSPF area.
Step 5	<p>mpls traffic-eng router-id <i>loopback0</i></p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng router-id loopback0</pre>	Specifies that the TE router identifier for the node is the IP address associated with interface loopback0.
Step 6	<p>exit</p> <p>Example:</p> <pre>Router(config-router)# exit</pre>	Exits to global configuration mode.
Step 7	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	Exits to privileged EXEC mode.

Configuring Traffic Engineering Link Metrics

Unless explicitly configured, the TE link metric is the IGP link metric. To configure the TE link metric, perform these steps:

SUMMARY STEPS

1. Router(config)# **interface** *interface*
2. Router(config-router)# **mpls traffic-eng administrative-weight** *weight*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# interface <i>interface</i>	Configures properties of the specified interface.
Step 2	Router(config-router)# mpls traffic-eng administrative-weight <i>weight</i>	Specifies the traffic engineering metric for the link.

Configuring an MPLS Traffic Engineering Tunnel

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

SUMMARY STEPS

1. Router(config)# **interface** *tunnel-interface*
2. Router(config-if)# **ip unnumbered loopback0**
3. Router(config-if)# **tunnel destination** *ip-address*
4. Router(config-if)# **tunnel mode mpls traffic-eng**
5. Router(config-if)# **tunnel mpls traffic-eng bandwidth** *bandwidth*
6. Router(config-if)# **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | **id** *path-number*}} [**lockdown**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	Router(config)# interface <i>tunnel-interface</i>	Configures a tunnel interface and enters interface configuration mode.
Step 2	Router(config-if)# ip unnumbered loopback0	Gives the tunnel interface an IP address. An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.

	Command or Action	Purpose
Step 3	Router(config-if)# tunnel destination <i>ip-address</i>	Specifies the destination for a tunnel. The destination must be the MPLS traffic engineering router ID of the destination device.
Step 4	Router(config-if)# tunnel mode mpls traffic-eng	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 5	Router(config-if)# tunnel mpls traffic-eng bandwidth <i>bandwidth</i>	Configures the bandwidth for the MPLS traffic engineering tunnel. If automatic bandwidth is configured for the tunnel, use the tunnel mpls traffic-eng bandwidth command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism.
Step 6	Router(config-if)# tunnel mpls traffic-eng path-option <i>number</i> { dynamic explicit { name <i>path-name</i> id <i>path-number</i> }} [lockdown]	Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database. A dynamic path is used if an explicit path is currently unavailable.

Configuring the Metric Type for Tunnel Path Calculation

Unless explicitly configured, the TE link metric type is used for tunnel path calculation. Two commands are provided for controlling the metric type to be used: an interface configuration command that specifies the metric type to be used for a particular TE tunnel and a global configuration command that specifies the metric type to be used for TE tunnels for which a metric type has not been specified by the interface configuration command.

To configure the metric type for tunnel path calculation, perform one or both of the following steps:

Command	Purpose
Router(config-if)# tunnel mpls traffic-eng path-selection metric { igp te }	Specifies the metric type to use for path calculation when you are determining a tunnel's path.
Router(config)# mpls traffic-eng path-selection metric { igp te }	Specifies the metric type to use if a metric type was not explicitly configured for a given tunnel.



Note

If you do not enter either of the commands, the traffic engineering (te) metric is used.

Verifying the Configuration

Use the **show mpls traffic-eng topology** command, which displays TE and IGP metrics for each link, to verify that link metrics have been correctly configured for a network.

```
Router# show mpls traffic-eng topology
My_System_id: 1440.0000.0044.00 (isis level-1)
IGP Id: 0090.0000.0009.00, MPLS TE Id:192.168.9.9 Router Node (isis level-1)
  link[0 ]:Nbr IGP Id: 0090.0000.0009.03, gen:7
    frag_id 0, Intf Address:10.0.0.99
    TE metric:100, IGP metric:48, attribute_flags:0x0      !!Note TE and IGP metrics
    physical_bw: 10000 (kbps), max_reservable_bw_global: 0 (kbps)
    max_reservable_bw_sub: 0 (kbps)
  .
  .
  link[1 ]:Nbr IGP Id: 0055.0000.0055.00, gen:7
    frag_id 0, Intf Address:10.205.0.9, Nbr Intf Address:10.205.0.55
    TE metric:120, IGP metric:10, attribute_flags:0x0      !!Note TE and IGP metrics
    physical_bw: 155000 (kbps), max_reservable_bw_global: 500000 (kbps)
    max_reservable_bw_sub: 0 (kbps)
  .
  .
  .
```

Use the **show mpls traffic-eng tunnels** command, which displays the link metric used for tunnel path calculation, to verify that the desired link metrics are being used for each tunnel.

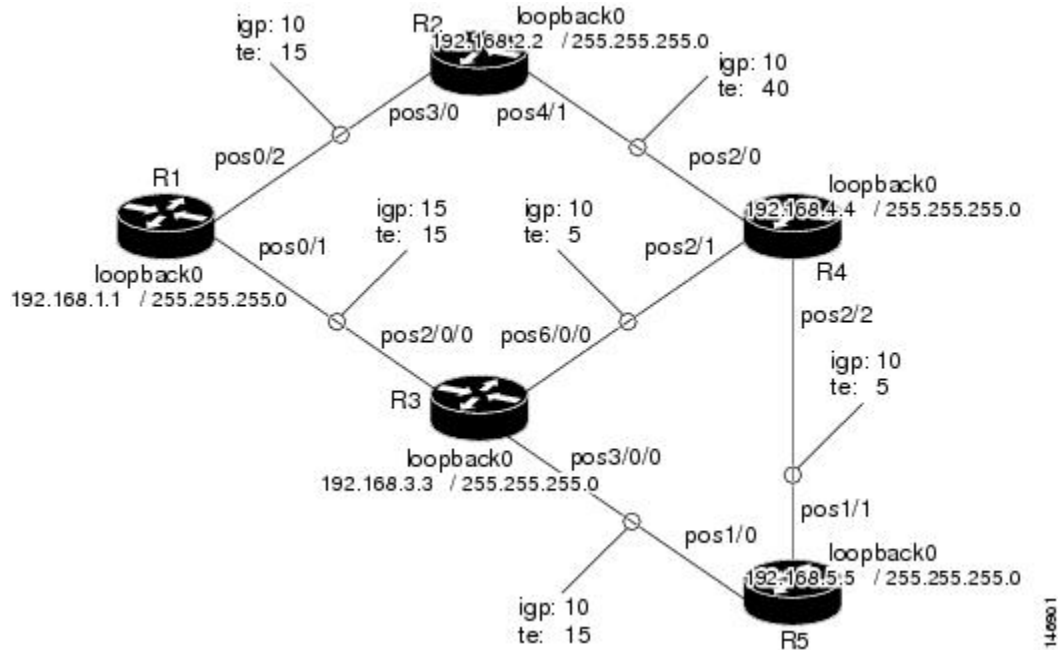
```
Router# show mpls traffic-eng tunnels
Name: te3640-17-c_t221 (Tunnel22) Destination: 192.168.100.22
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, type dynamic (Basis for Setup, path weight 10)
Config Parameters:
  Bandwidth: 400 kps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
  Metric Type: IGP !!Note metric type
  AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled(0/115) 0 Bandwidth Requested: 0
.
.
Name: te3640-17-c_t222 (Tunnel33) Destination: 192.168.100.22
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, type dynamic (Basis for Setup, path weight 10)
Config Parameters:
  Bandwidth: 200 kbps (Global) Priority: 1 1 Affinity: 0x0/0xFFFF
  Metric Type: TE !!Note metric type
  AutoRoute: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled(0/115) 0 Bandwidth Requested: 0
.
.
.
```

Configuration Examples

The section illustrates how to configure the link metric type to be used for tunnel path selection, and how to configure the link metrics themselves. The configuration commands included focus on specifying the metric type for path calculation and assigning metrics to links. Additional commands are required to fully configure the example scenario: for example, the IGP commands for traffic engineering and the link interface commands for enabling traffic engineering and specifying available bandwidth.

The examples in this section support the simple network topology shown in the figure below.

Figure 4: Network Topology



In the figure above:

- Tunnel1 and Tunnel2 run from R1 (headend) to R4 (tailend).
- Tunnel3 runs from R1 to R5.
- Path calculation for Tunnel1 and Tunnel3 should use a metric that represents link delay because these tunnels carry voice traffic.
- Path calculation for Tunnel2 should use IGP metrics because MPLS TE carries data traffic with no delay requirement.

Configuration fragments follow for each of the routers that illustrate the configuration relating to link metrics and their use in tunnel path calculation. TE metrics that represent link delay must be configured for the network links on each of the routers, and the three tunnels must be configured on R1.

These configuration fragments force Tunnel1 to take path R1-R3-R4, Tunnel2 to take path R1-R2-R4, and Tunnel3 to take path R1-R3-R4-R5 (assuming the links have sufficient bandwidth to accommodate the tunnels).

R1 Configuration

```
interface pos0/1
mpls traffic-eng administrative-weight 15           !TE metric different from IGP metric
interface pos0/2
mpls traffic-eng administrative-weight 15           !TE metric different from IGP metric
interface Tunnel1
                                                    !Tunnel1 uses TE metric (default)
                                                    !for path selection

ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
```

```

tunnel mpls traffic-eng path-option 1 dynamic
interface Tunnel2                                !Tunnel2 uses IGP metric
                                                !for path selection

ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng path-selection-metric igp !Use IGP cost for path selection.
interface Tunnel3                                !Tunnel3 uses TE metric (default)
                                                !for path selection

ip unnumbered loopback0
tunnel destination 192.168.5.5 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic

```

R2 Configuration

```

interface pos3/0
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos4/1
mpls traffic-eng administrative-weight 40        !TE metric different from IGP metric

```

R3 Configuration

```

interface pos2/0/0
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos3/0/0
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos6/0/0
mpls traffic-eng administrative-weight 5         !TE metric different from IGP metric

```

R4 Configuration

```

interface pos2/0
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos2/1
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos2/2
mpls traffic-eng administrative-weight 5         !TE metric different from IGP metric

```

R5 Configuration

```

interface pos1/0
mpls traffic-eng administrative-weight 15        !TE metric different from IGP metric
interface pos1/1
mpls traffic-eng administrative-weight 5         !TE metric different from IGP metric

```

Additional References

Related Document

Related Topic	Document Title
MPLS Traffic Engineering Path Protection	MPLS Traffic Engineering Path Protection

Related Topic	Document Title
MPLS Traffic Engineering--Fast Reroute Link and Node Protection	MPLS Traffic Engineering--Fast Reroute Link and Node Protection

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

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>http://www.cisco.com/techsupport</p>

Feature Information for MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2: Feature Information for MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels

Feature Name	Releases	Feature Information
MPLS Traffic Engineering:Configurable Path Calculation Metric for Tunnels	12.0(18)ST 12.2(11)S 12.2(14)S 12.2(28)SB 12.4(20)T Cisco IOS XE Release 2.3	<p>The MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels feature enables the user to control the metric used in path calculation for traffic engineering (TE) tunnels on a per-tunnel basis. Certain tunnels are used to carry voice traffic, which requires low delay, and other tunnels are used to carry data. A TE link metric can be used to represent link delay and configure tunnels that carry voice traffic for path calculation and configure tunnels that carry data to use the Interior Gateway Protocol (IGP) metric for path calculation.</p> <p>The following commands were introduced or modified: mpls traffic-eng path-selection metric, tunnel mpls traffic-eng path-selection metric.</p>



MPLS Traffic Engineering Scalability Enhancements

The MPLS Traffic Engineering: Scalability Enhancement feature improves scalability performance for large numbers of traffic engineering tunnels.

These improvements allow an increase in the number of traffic engineering (TE) tunnels a router can support when the router is configured as a tunnel headend. Additionally, when the router is configured as a tunnel midpoint, the enhancements reduce the time required to establish large numbers of TE tunnels.

This feature module contains information about and instructions on how to configure the Multiprotocol Label Switching (MPLS) traffic engineering scalability enhancements.

- [Finding Feature Information, page 45](#)
- [Prerequisites for MPLS Traffic Engineering Scalability Enhancements, page 46](#)
- [Restrictions for MPLS Traffic Engineering Scalability Enhancements, page 46](#)
- [Information About MPLS Traffic Engineering Scalability Enhancements, page 46](#)
- [How to Configure MPLS Traffic Engineering Scalability Enhancements, page 48](#)
- [Configuration Examples for MPLS Traffic Engineering Scalability Enhancements, page 55](#)
- [Additional References, page 56](#)
- [Feature Information for MPLS Traffic Engineering Scalability Enhancements, page 58](#)
- [Glossary, page 59](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering Scalability Enhancements

Your network must support the following Cisco IOS features before you enable MPLS traffic engineering:

- MPLS
- Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

Restrictions for MPLS Traffic Engineering Scalability Enhancements

The number of tunnels that a particular platform can support can vary depending on:

- The types of interfaces that the tunnels traverse
- The manner in which the Resource Reservation Protocol (RSVP) message pacing feature is configured
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

Information About MPLS Traffic Engineering Scalability Enhancements

Scalability Enhancements for Traffic Engineering Tunnels

Scalability performance is improved for large numbers of traffic engineering tunnels, and includes the following enhancements:

- Increase the number of traffic engineering tunnels a router can support when configured as a tunnel headend and when configured as a tunnel midpoint
- Reduce the time required to establish large numbers of traffic engineering tunnels

RSVP Rate Limiting

A burst of RSVP traffic engineering signaling messages can overflow the input queue of a receiving router, causing some messages to be dropped. Dropped messages cause a substantial delay in completing label switched path (LSP) signaling.

This MPLS Traffic Engineering--Scalability Enhancements feature provides an enhancement mechanism that controls the transmission rate for RSVP messages and reduces the likelihood of input drops on the receiving router. The default transmission rate is 200 RSVP messages per second to a given neighbor. The rate is configurable.

Improved Recovery Response for Signaling and Management of MPLS Traffic Engineering Tunnels

The MPLS Traffic Engineering--Scalability Enhancements feature improves the recovery response for signaling and management of MPLS TE tunnels. LSP recovery responsiveness is improved when a link used by an LSP fails:

- When the upstream end of a failed link detects the failure, the software generates an RSVP No Route path error message. This enables the LSP headend to detect the link failure and initiate recovery, even when the Interior Gateway Protocol (IGP) update announcing the link failure is delayed.
- The LSP headend marks the link in question so that subsequent constraint-based shortest path first (SPF) calculations ignore the link until either a new IGP update arrives or a configurable timeout occurs. This ensures that resignaling to restore the LSP avoids the failed link.

IS-IS and MPLS Traffic Engineering Topology Database Interactions

The MPLS Traffic Engineering--Scalability Enhancements feature reduces the interval between when the IS-IS protocol receives an IGP update and when it delivers the update to the MPLS traffic engineering topology database.

Before the MPLS Traffic Engineering--Scalability Enhancements feature was introduced, when IS-IS received a new LSP that contained traffic engineering type, length, value (TLV) objects, a delay of several seconds could occur before IS-IS passed the traffic engineering TLVs to the traffic engineering database. The purpose of the delay was to provide better scalability during periods of network instability and to give the router an opportunity to receive more fragments of the LSP before passing the information to the traffic engineering database. However, this delay increased the convergence time for the traffic engineering database.

With the MPLS Traffic Engineering--Scalability Enhancements feature, IS-IS extracts traffic engineering TLVs from received LSPs and passes them to the traffic engineering database immediately. The exception to this occurs when there are large numbers of LSPs to process and it is important to limit CPU consumption, such as during periods of network instability. The parameters that control IS-IS delivery of traffic engineering TLVs to the traffic engineering topology database are configurable.

**Note**

MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

Improved Counter Capabilities for MPLS TE Tunnels Events and RSVP Signaling

With the MPLS Traffic Engineering--Scalability Enhancements feature, diagnostic and troubleshooting capabilities for MPLS traffic engineering tunnels and RSVP are improved:

- Counters record tunnel headend error events such as no route (link down), preemption, and insufficient bandwidth on a per-tunnel basis.
- Counters record RSVP messages. The counters are per-interface and record the number of RSVP messages of each type sent and received on the interface.

Benefits of MPLS Traffic Engineering Scalability Enhancements

The MPLS Traffic Engineering--Scalability Enhancements feature provides the following benefits:

- Increased scalability: Up to 600 MPLS traffic engineering tunnel headends are supported. Up to 10,000 traffic engineering tunnel midpoints are supported, with up to 5000 midpoints per interface.
- Faster recovery after failure conditions: Message pacing provides a mechanism to throttle RSVP control messages so that they are less likely to be dropped. This results in a faster recovery from failure conditions when many MPLS traffic engineering tunnels are being set up.
- Improved reroute time: When a traffic engineering tunnel is down, the headend router needs to be notified so that it can signal for a new LSP for the tunnel along an alternate path. The headend router does not have to wait for an IGP update to signal for a new LSP for the tunnel along an alternate path.
- Improved tunnel setup time: Fewer control messages and tunnel setup messages are dropped. This reduces the average time required to set up tunnels.

How to Configure MPLS Traffic Engineering Scalability Enhancements

Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements

Perform the following task to enable RSVP rate limiting for MPLS traffic engineering scalability enhancements. RSVP rate limiting maintains, on an outgoing interface basis, a count of messages that were dropped because the output queue for the interface used for rate limiting was full.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling rate-limit [burst number] [limit number] [maxsize bytes] [period ms]**
4. **end**
5. **show ip rsvp neighbor**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>ip rsvp signalling rate-limit [burst number] [limit number] [maxsize bytes] [period ms]</p> <p>Example:</p> <pre>Router(config)# ip rsvp signalling rate-limit burst 5 maxsize 3 period 2</pre>	<p>Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.</p> <ul style="list-style-type: none"> • The burst number keyword and argument pair indicates the maximum number of RSVP messages sent to a neighboring router during each interval. The range is from 1 to 5000. The default is 8. • The limit number keyword and argument pair indicates the maximum number of messages to send per queue interval when the number of messages sent is less than the number of messages to be sent normally. The range is from 1 to 5000. The default is 37. • The maxsize bytes keyword and argument pair indicates the maximum size of the message queue, in bytes. The range is from 1 to 5000. The default is 2000. • The period ms keyword and argument pair indicates the length of the interval (time frame) in milliseconds (ms). The range is from 10 to 5000. The default is 20.
Step 4	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	<p>Exits to privileged EXEC mode.</p>
Step 5	<p>show ip rsvp neighbor</p> <p>Example:</p> <pre>Router# show ip rsvp neighbor</pre>	<p>Displays current RSVP neighbors.</p> <p>Use this command to verify that RSVP message pacing is enabled.</p>

Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels

Perform this task to manage link failure timeouts for MPLS traffic engineering tunnels.

This allows the configuration of a timeout during which the router ignores a link in its path calculation to avoid paths that contain a failed link and are likely to fail when signaled.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng topology holddown sigerr *seconds***
4. **end**
5. **show mpls traffic-eng topology [brief]**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	mpls traffic-eng topology holddown sigerr <i>seconds</i> Example: Router(config)# mpls traffic-eng topology holddown sigerr 15	Specifies the amount of time that a router ignores a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link. <ul style="list-style-type: none"> • The <i>seconds</i> argument specifies the length of time (in seconds) a router should ignore a link during tunnel path calculations following a traffic engineering tunnel error on the link. The value can be from 0 to 300. The default is 10.
Step 4	end Example: Router(config)# end	Exits to privileged EXEC mode.

	Command or Action	Purpose
Step 5	show mpls traffic-eng topology [brief] Example: <pre>Router# show mpls traffic-eng topology brief</pre>	Displays the MPLS traffic engineering global topology as currently known at this node. <ul style="list-style-type: none"> The brief keyword provides a less detailed version of the topology.

Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database

Perform the following task to control IS-IS and MPLS traffic engineering topology database interactions. This reduces the interval time between when the IS-IS protocol receives an IGP update and when IS-IS delivers the update to the MPLS traffic engineering topology database, which reduces convergence time for the database.



Note

MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis [area-tag]**
4. **mpls traffic-eng scanner [interval seconds] [max-flash LSPs]**
5. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	<p>router isis [<i>area-tag</i>]</p> <p>Example:</p> <pre>Router(config)# router isis</pre>	<p>Enables the IS-IS routing protocol and specifies an IS-IS process.</p> <ul style="list-style-type: none"> The <i>area-tag</i> argument is a meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router. <p>Note This argument is Required for multiarea IS-IS configuration and optional for conventional IS-IS configuration.</p>
Step 4	<p>mpls traffic-eng scanner [<i>interval seconds</i>] [max-flash <i>LSPs</i>]</p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng scanner interval 5 max-flash 100</pre>	<p>Specifies how often IS-IS extracts traffic engineering TLVs from flagged LSPs and passes them to the traffic engineering topology database, and specifies the maximum number of LSPs that the router can process immediately.</p> <ul style="list-style-type: none"> The interval <i>seconds</i> keyword and argument specify the frequency, in seconds, at which IS-IS sends traffic engineering TLVs into the traffic engineering database. The value can be from 1 to 60. The default value is 5. The max-flash <i>LSPs</i> keyword and argument specify the maximum number of LSPs that the router can process immediately without incurring a delay. The value can be from 0 to 200. The default value is 15.
Step 5	<p>end</p> <p>Example:</p> <pre>Router(config-router)# end</pre>	<p>Exits to privileged EXEC mode.</p>

Monitoring and Maintaining MPLS TE Scalability Enhancements

SUMMARY STEPS

1. **enable**
2. **show ip rsvp neighbor** [*detail*]
3. **show ip rsvp counters** [*summary*]
4. **clear ip rsvp counters**
5. **clear ip rsvp signalling rate-limit**
6. **show mpls traffic-eng tunnels statistics**
7. **clear mpls traffic-eng tunnels counters**
8. **show mpls traffic-eng topology** [*brief*]
9. **exit**

DETAILED STEPS

Step 1 enable

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

Example:

```
Router> enable
Router#
```

Step 2 show ip rsvp neighbor [detail]

Use this command to verify that RSVP message pacing is turned on. For example:

Example:

```
Router# show ip rsvp neighbor detail
Neighbor:10.0.0.1
  Encapsulation:RSVP
  Rate-Limiting:
    Dropped messages:0
  Refresh Reduction:
    Remote epoch:0x1BFEA5
    Out of order messages:0
    Retransmitted messages:0
    Highest rcvd message id:1059
    Last rcvd message:00:00:04
Neighbor:10.0.0.2
  Encapsulation:RSVP
  Rate-Limiting:
    Dropped messages:0
  Refresh Reduction:
    Remote epoch:0xB26B1
    Out of order messages:0
    Retransmitted messages:0
    Highest rcvd message id:945
    Last rcvd message:00:00:05
```

Step 3 show ip rsvp counters [summary]

Use this command to display the counts of RSVP messages that were sent and received. For example:

Example:

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit
Path                   110       15   Resv                50       28
PathError              0         0   ResvError           0         0
PathTear               0         0   ResvTear            0         0
ResvConf               0         0   RTearConf           0         0
Ack                    0         0   Srefresh            0         0
Hello                  5555      5554  IntegrityChalle     0         0
IntegrityRespon       0         0   DSBM_WILLING        0         0
I_AM_DSBM              0         0
Unknown               0         0   Errors              0         0
Recv Msg Queues       Current   Max
RSVP                   0         2
Hello (per-I/F)       0         1
Awaiting Authentication 0         0
```

Step 4 clear ip rsvp counters

Use this command to clear (set to zero) all IP RSVP counters that are being maintained. For example:

Example:

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

Step 5 clear ip rsvp signalling rate-limit

Use this command to clear (set to zero) counts of the messages that message pacing was forced to drop because the output queue for the interface used for message pacing was full. For example:

Example:

```
Router# clear ip rsvp signalling rate-limit
```

Step 6 show mpls traffic-eng tunnels statistics

Use this command to display event counters for one or more MPLS traffic engineering tunnels. For example:

Example:

```
Router# show mpls traffic-eng tunnels statistics
Tunnel1001 (Destination 10.8.8.8; Name Router_t1001)
  Management statistics:
    Path: 25 no path, 1 path no longer valid, 0 missing ip exp path
  5 path changes
    State: 3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens: 2 succeeded, 0 timed out, 0 bad path spec
  0 other aborts
    Errors: 0 no b/w, 0 no route, 0 admin
  0 bad exp route, 0 rec route loop, 0 other
...

```

Example:

```
Tunnel17050 (Destination 10.8.8.8; Name Router_t7050)
  Management statistics:
    Path: 19 no path, 1 path no longer valid, 0 missing ip exp path
  3 path changes
    State: 3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens: 2 succeeded, 0 timed out, 0 bad path spec
  0 other aborts
    Errors: 0 no b/w, 0 no route, 0 admin
  0 bad exp route, 0 rec route loop, 0 other

```

Step 7 clear mpls traffic-eng tunnels counters

Use this command to clear counters for all MPLS traffic engineering tunnels. For example:

Example:

```
Router# clear mpls traffic-eng tunnels counters
Clear traffic engineering tunnel counters [confirm]
```

Step 8 show mpls traffic-eng topology [brief]

Use this command to display the MPLS traffic engineering topology database. For example:

Example:

```
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 9**exit**

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

Example:

```
Router# exit
Router>
```

Configuration Examples for MPLS Traffic Engineering Scalability Enhancements

Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements Examples

The following examples show how to enable RSVP rate limiting for MPLS traffic engineering scalability enhancements:

```
configure terminal
 ip rsvp signalling rate-limit
end
```

The following is sample output that traffic engineering displays when RSVP rate limiting is enabled:

```
Router# show ip rsvp signalling rate-limit
Rate Limiting: enabled
  Burst: 10
  Limit: 37
  Maxsize: 5000
  Period (msec): 100
  Max rate (msgs/sec): 100
```

The following example shows how to configure a router to send a maximum of 5 RSVP traffic engineering signaling messages in 1 second to a neighbor. The size of the output queue is 35.

```
configure terminal
 ip rsvp signalling rate-limit
 period 1 burst 5 maxsize 35
```

Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels Example

The following example shows how to manage link failure timeouts for MPLS traffic engineering tunnels:

```
configure terminal
mpls traffic-eng topology holddown sigerr 15
end
```

In this example, the link hold-down time for signaling errors is set to 15 seconds.

Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database Example

The following example shows how to control IS-IS communication with the MPLS traffic engineering topology database:

```
configure terminal
router isis
mpls traffic-eng scanner interval 5 max-flash 50
end
```

In this example, the router is enabled to process up to 50 IS-IS LSPs without any delay.

Additional References

The following sections provide references related to the MPLS Traffic Engineering (TE): Scalability Enhancements feature.

Related Documents

Related Topic	Document Title
Quality of service	<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i>
MPLS	<ul style="list-style-type: none"> • <i>Cisco IOS Multiprotocol Label Switching Command Reference</i> • <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</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
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: http://www.cisco.com/go/mibs

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>	http://www.cisco.com/techsupport

Feature Information for MPLS Traffic Engineering Scalability Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 3: Feature Information for MPLS Traffic Engineering Scalability Enhancements

Feature Name	Releases	Feature Information
MPLS Traffic Engineering: Scalability Enhancements	12.0(14)ST 12.2(14)S 12.0(22)S 12.2(28)SB 12.4(20)T	<p>The MPLS Traffic Engineering: Scalability Enhancements feature improves scalability performance for large numbers of traffic engineering tunnels.</p> <p>These improvements allow an increase in the number of traffic engineering (TE) tunnels a router can support when the router is configured as a tunnel headend. Additionally, when the router is configured as a tunnel midpoint, the enhancements reduce the time required to establish large numbers of TE tunnels.</p> <p>This feature module contains information about and instructions on how to configure the Multiprotocol Label Switching (MPLS) traffic engineering scalability enhancements.</p> <p>The following commands were introduced or modified: clear ip rsvp counters, clear ip rsvp signalling rate-limit, clear mpls traffic-eng tunnel counters, ip rsvp signalling rate-limit, mpls traffic-eng scanner, mpls traffic-eng topology holddown sigerr, show ip rsvp counters, and show mpls traffic-eng tunnels statistics.</p>

Glossary

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.

CLNS --Connectionless Network Services. The Open System Interconnection (OSI) network layer service that does not require a circuit to be established before the data is transmitted. CLNS routes messages to their destination independently of any other messages.

CSPF --Constrained Shortest Path First. A routing protocol that calculates the shortest path based on a set of constraints, such as a minimum bandwidth requirement, maximum number of nodes, or nodes to include or exclude.

enterprise network --A large and diverse network connecting most major points in a company or other organization.

headend --The endpoint of a broadband network. All stations send toward the headend; the headend then sends toward the destination stations.

IGP --Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include IGRP, OSPF, and RIP.

interface --A network connection.

IS-IS --Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where ISs (routers) exchange routing information based on a single metric, to determine the network topology.

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.

message-pacing --The former name of the rate limiting feature.

MPLS --Multiprotocol Label Switching (formerly known as tag switching). A method for directing packets primarily through Layer 2 switching rather than Layer 3 routing. In MPLS, packets are assigned short fixed-length labels at the ingress to an MPLS cloud by 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.

OSPF --Open Shortest Path First. A link-state, hierarchical Interior Gateway Protocol (IGP) routing protocol derived from the Intermediate System-Intermediate System (IS-IS) protocol. OSPF features are 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.

RSVP --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network.

scalability --An indicator showing how quickly some measure of resource usage increases as a network gets larger.

TLV --type, length, value objects. TLVs are used in data communication to provide optional information. The type field indicates the type of items in the value field. The length field indicates the length of the value field. The value field is the data portion of the packet.

topology --The physical arrangement of network nodes and media within an enterprise networking structure.

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.

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.



MPLS Traffic Engineering--LSP Attributes

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, page 61](#)
- [Prerequisites for MPLS Traffic Engineering--LSP Attributes, page 62](#)
- [Restrictions for MPLS Traffic Engineering--LSP Attributes, page 62](#)
- [Information About MPLS Traffic Engineering--LSP Attributes, page 62](#)
- [How to Configure MPLS Traffic Engineering--LSP Attributes, page 66](#)
- [Configuration Examples for MPLS Traffic Engineering--LSP Attributes, page 94](#)
- [Additional References, page 98](#)
- [Feature Information for MPLS Traffic Engineering LSP Attributes, page 100](#)
- [Glossary, page 101](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

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

MPLS Traffic Engineering--LSP Attributes Benefits

The MPLS Traffic Engineering--LSP Attributes feature 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 Attribute 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 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

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 (**noattribute** 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

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).

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. The **tunnel mpls traffic-eng path-option** command's **bandwidth** keyword can be used for this purpose. 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 tunnel's configured bandwidth.

This feature also provides 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 uses the **tunnel mpls traffic-eng bandwidth** command to configure the bandwidth of the tunnel and three **tunnel mpls traffic-eng path-option** commands that define the signalling path options for the LSP:

```
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

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

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* [*maskvalue*]
5. **auto-bw** [*frequencysecs*] [*max-bwkbps*] [*min-bwkbps*] [*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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>mpls traffic-eng lsp attributes <i>string</i></p> <p>Example:</p> <pre>Router(config)# mpls traffic-eng lsp attributes 1</pre>	<p>Configures an LSP Attribute list and enters LSP Attribute configuration mode.</p> <ul style="list-style-type: none"> • The <i>string</i> argument identifies a specific LSP Attribute list.
Step 4	<p>affinity <i>value</i> [<i>maskvalue</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# affinity 0 mask 0</pre>	<p>(Optional) Specifies attribute flags for links comprising an LSP.</p> <ul style="list-style-type: none"> • 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. • The maskvalue keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> • If a bit in the mask is 0, an attribute value of the link for that bit is irrelevant. • 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.
Step 5	<p>auto-bw [<i>frequencysecs</i>] [<i>max-bwkbps</i>] [<i>min-bwkbps</i>] [<i>collect-bw</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# auto-bw</pre>	<p>(Optional) Specifies automatic bandwidth configuration.</p> <ul style="list-style-type: none"> • The frequencysecs keyword argument combination specifies the interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. • The max-bwkbps keyword argument combination specifies the maximum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295. • The min-bwkbps keyword argument combination specifies the minimum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295. • The collect-bw keyword collects output rate information for the path option, but does not adjust the bandwidth of the path option.

	Command or Action	Purpose
Step 6	<p>bandwidth [sub-pool global] <i>kbps</i></p> <p>Example:</p> <pre>Router(config-lsp-attr)# bandwidth 5000</pre>	<p>(Optional) Specifies LSP bandwidth.</p> <ul style="list-style-type: none"> • The sub-pool keyword indicates a subpool path option. • The global 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 sub-pool keyword. • 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.
Step 7	<p>list</p> <p>Example:</p> <pre>Router(config-lsp-attr)# list</pre>	<p>(Optional) Displays the contents of the LSP attribute list.</p>
Step 8	<p>lockdown</p> <p>Example:</p> <pre>Router(config-lsp-attr)# lockdown</pre>	<p>(Optional) Disables reoptimization of the LSP.</p>
Step 9	<p>priority <i>setup-priority</i> [<i>hold-priority</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# priority 1 1</pre>	<p>(Optional) Specifies the LSP priority.</p> <ul style="list-style-type: none"> • 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. • 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.
Step 10	<p>protection fast-reroute</p> <p>Example:</p> <pre>Router(config-lsp-attr)# protection fast-reroute</pre>	<p>(Optional) Enables failure protection on the LSP.</p>
Step 11	<p>record-route</p> <p>Example:</p> <pre>Router(config-lsp-attr)# record-route</pre>	<p>(Optional) Records the route used by the LSP.</p>
Step 12	<p>no <i>sub-command</i></p>	<p>(Optional) Removes a specific attribute from the LSP attributes list.</p>

	Command or Action	Purpose
	Example: <pre>Router(config-lsp-attr)# no record-route</pre>	<ul style="list-style-type: none"> The <i>sub-command</i> argument names the LSP attribute to remove from the attributes list.
Step 13	exit Example: <pre>Router(config-lsp-attr)# exit</pre>	(Optional) Exits from LSP Attribute configuration mode.
Step 14	end Example: <pre>Router(config)# end</pre>	(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* [*maskvalue*]
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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>mpls traffic-eng lsp attributes <i>string</i></p> <p>Example:</p> <pre>Router(config)# mpls traffic-eng lsp attributes 1</pre>	<p>Configures an LSP Attribute list and enters LSP Attributes configuration mode.</p> <ul style="list-style-type: none"> The <i>string</i> argument identifies a specific LSP Attribute list.
Step 4	<p>affinity <i>value</i> [<i>maskvalue</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# affinity 0 mask 0</pre>	<p>(Optional) Specifies attribute flags for links comprising an LSP.</p> <ul style="list-style-type: none"> 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. The maskvalue keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match.
Step 5	<p>bandwidth [<i>sub-pool</i> <i>global</i>] <i>kbps</i></p> <p>Example:</p> <pre>Router(config-lsp-attr)# bandwidth 1000</pre>	<p>Specifies an LSP bandwidth.</p> <ul style="list-style-type: none"> The sub-pool keyword indicates a subpool path option. The global 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 sub-pool keyword. 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.
Step 6	<p>priority <i>setup-priority</i> [<i>hold-priority</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# priority 2 2</pre>	<p>Specifies the LSP priority.</p> <ul style="list-style-type: none"> 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. 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.

	Command or Action	Purpose
Step 7	list Example: Router(config-lsp-attr)# list	(Optional) Displays the contents of the LSP attribute list. <ul style="list-style-type: none"> • Use the list command to display the path option attributes added to the attribute list.
Step 8	exit Example: Router(config-lsp-attr)# exit	(Optional) Exits LSP Attributes configuration mode.
Step 9	end Example: 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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>mpls traffic-eng lsp attributes <i>string</i></p> <p>Example:</p> <pre>Router(config)# mpls traffic-eng lsp attributes 1</pre>	<p>Configures an LSP Attribute list and enters LSP Attributes configuration mode.</p> <ul style="list-style-type: none"> The <i>string</i> argument identifies a specific LSP attribute list.
Step 4	<p>no <i>sub-command</i></p> <p>Example:</p> <pre>Router(config-lsp-attr)# no priority</pre>	<p>Removes a specific attribute from the LSP Attribute list.</p> <ul style="list-style-type: none"> The <i>sub-command</i> argument names the LSP attribute to remove from the attributes list.
Step 5	<p>list</p> <p>Example:</p> <pre>Router(config-lsp-attr)# list</pre>	<p>(Optional) Displays the contents of the LSP attribute list.</p> <ul style="list-style-type: none"> Use the list command to verify that the path option attribute is removed from the attribute list.
Step 6	<p>exit</p> <p>Example:</p> <pre>Router(config-lsp-attr)# exit</pre>	(Optional) Exits LSP Attributes configuration mode.
Step 7	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	(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* [**maskvalue**]
5. **list**
6. **affinity** *value* [**maskvalue**]
7. **list**
8. **exit**
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	mpls traffic-eng lsp attributes <i>string</i> Example: 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"> • The <i>string</i> argument identifies a specific LSP attribute list.
Step 4	affinity <i>value</i> [maskvalue] Example: Router(config-lsp-attr)# affinity 1 mask 1	Specifies attribute flags for links comprising an LSP. <ul style="list-style-type: none"> • The <i>value</i> argument is a value required for links comprising an LSP. Values of bits are either 0 or 1. • The maskvalue keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> • If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. • If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.
Step 5	list	(Optional) Displays the contents of the LSP Attribute list.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-lsp-attr)# list</pre>	<ul style="list-style-type: none"> Use the list command to display the path option attributes configured in the attribute list.
Step 6	<p>affinity <i>value</i> [<i>maskvalue</i>]</p> <p>Example:</p> <pre>Router(config-lsp-attr)# affinity 0 mask 0</pre>	<p>Specifies attribute flags for links comprising an LSP.</p> <ul style="list-style-type: none"> The <i>value</i> argument is a value required for links comprising an LSP. Values of bits are either 0 or 1. The maskvalue keyword argument combination indicates which attribute values should be checked. <ul style="list-style-type: none"> If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant. If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match.
Step 7	<p>list</p> <p>Example:</p> <pre>Router(config-lsp-attr)# list</pre>	<p>(Optional) Displays the contents of the LSP attribute list.</p> <ul style="list-style-type: none"> Use the list command to verify that the path option attributes is modified in the attribute list.
Step 8	<p>exit</p> <p>Example:</p> <pre>Router(config-lsp-attr)# exit</pre>	<p>(Optional) Exits LSP Attributes configuration mode.</p>
Step 9	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	<p>(Optional) Exits to privileged EXEC mode.</p>

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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>no mpls traffic-eng lsp attributes <i>string</i></p> <p>Example:</p> <pre>Router(config)# no mpls traffic-eng lsp attributes 1</pre>	<p>Removes a specified LSP Attribute list from the device configuration.</p> <ul style="list-style-type: none"> • The <i>string</i> argument identifies the specific LSP attribute list to remove.
Step 4	<p>end</p> <p>Example:</p> <pre>Router(config)# end</pre>	<p>(Optional) Exits to privileged EXEC mode.</p>
Step 5	<p>show mpls traffic-eng lsp attributes [<i>string</i>]</p> <p>Example:</p> <pre>Router# show mpls traffic-eng lsp attributes</pre>	<p>(Optional) Displays information about configured LSP attribute lists.</p> <ul style="list-style-type: none"> • Use the show mpls traffic-eng lsp attributes command to verify that the LSP attribute list was deleted from the router.

Verifying 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**enable**

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

Example:

```
Router> enable
Router#
```

Step 2**configure terminal**

Use this command to enter global configuration mode. For example:

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:

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
```

Example:

```
Router(config)#
```

Step 5**end**

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

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:

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:

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 **show mpls traffic-eng lsp *text-string*** to locate the LSP attributes information in the configuration file. For example:

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:

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.

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*] *bandwidth*
8. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
9. **tunnel mpls traffic-eng path-option** *number* **{dynamic | explicit** *{namepath-name | path-number}* [*verbatim*]} [*attributes string*] [*bandwidth* [*sub-pool | global*] *kbps*] [*lockdown*]
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface tunnel 1	Configures an interface type and enters interface configuration mode. • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	tunnel destination <i>{hostname ip-address}</i>	Specifies the destination of the tunnel for this path option. • The <i>hostname</i> argument is the name of the host destination.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-if)# tunnel destination 10.10.10.12</pre>	<ul style="list-style-type: none"> The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the encapsulation mode for the tunnel for MPLS TE.
Step 6	<p>tunnel mpls traffic-eng autoroute announce</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng autoroute announce</pre>	Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.
Step 7	<p>tunnel mpls traffic-eng bandwidth [sub-pool global] bandwidth</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 1000</pre>	<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"> The sub-pool keyword indicates a subpool tunnel. The global 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 sub-pool keyword. 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.
Step 8	<p>tunnel mpls traffic-eng priority setup-priority [hold-priority]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng priority 1 1</pre>	<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"> 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. <p>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.</p> <ul style="list-style-type: none"> 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. <p>Valid values are from 0 to 7, where a lower number indicates a higher priority.</p>
Step 9	<p>tunnel mpls traffic-eng path-option number {dynamic explicit {namepath-name path-number} [verbatim]} [attributes string]</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"> The <i>number</i> argument identifies the path option.

	Command or Action	Purpose
	<p>[bandwidth [sub-pool global] <i>kbps</i>] [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1</pre> <p>Example:</p>	<ul style="list-style-type: none"> • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path. • The namepath-name keyword argument combination identifies the name of the explicit path option. • The <i>path-number</i> argument identifies the number of the explicit path option. • The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> • The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. • The bandwidth keyword specifies LSP bandwidth. • The sub-pool keyword indicates a subpool path option. • The global 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 sub-pool keyword. • 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. • The lockdown keyword disables reoptimization of the LSP.
Step 10	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits to privileged EXEC mode.

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. The **tunnel mpls traffic-eng path-option number dynamic attributes string** command is used in interface configuration mode to modify the path option to use a different LSP attribute list. The **attributes** and *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 {namepath-name | path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool | global] kbps] [lockdown]*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface tunnel 1	Configures the interface type and enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	tunnel destination <i>{hostname ip-address}</i> Example: 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"> • The <i>hostname</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	tunnel mpls traffic-eng path-option <i>number {dynamic explicit {namepath-name path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool global] kbps] [lockdown]</i> Example: Router(config-if)# tunnel mpls	Adds an LSP Attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel. <ul style="list-style-type: none"> • The <i>number</i> argument identifies the path option. • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path.

	Command or Action	Purpose
	<pre>traffic-eng path-option 1 dynamic attributes 1</pre>	<ul style="list-style-type: none"> The namepath-name keyword argument combination identifies the name of the explicit path option. The <i>path-number</i> argument identifies the number of the explicit path option. The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. The bandwidth keyword specifies LSP bandwidth. The sub-pool keyword indicates a subpool path option. The global 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 sub-pool keyword. 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. The lockdown keyword disables reoptimization of the LSP.
Step 6	<pre>end</pre> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits to privileged EXEC mode.

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** {*namepath-name* | *path-number*} [**verbatim**]} [**attributesstring**] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p>interface <i>type number</i></p> <p>Example:</p> <pre>Router(config)# interface tunnel 1</pre>	<p>Configures the interface type and enters interface configuration mode.</p> <ul style="list-style-type: none"> • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	<p>tunnel destination {<i>hostname</i> <i>ip-address</i>}</p> <p>Example:</p> <pre>Router(config-if)# tunnel destination 10.10.10.12</pre>	<p>Specifies the destination of the tunnel for this path option.</p> <ul style="list-style-type: none"> • The <i>hostname</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	<p>no tunnel mpls traffic-eng path-option <i>number</i> {dynamic explicit {<i>namepath-name</i> <i>path-number</i>} [verbatim]} [attributesstring] [bandwidth [sub-pool global] <i>kbps</i>] [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# no tunnel mpls traffic-eng path-option 1 dynamic attributes 1</pre>	<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"> • The <i>number</i> argument identifies the path option. • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path. • The namepath-name keyword argument combination identifies the name of the explicit path option. • The <i>path-number</i> argument identifies the number of the explicit path option. • The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> • The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. • The bandwidth keyword specifies LSP bandwidth.

	Command or Action	Purpose
		<ul style="list-style-type: none"> • The sub-pool keyword indicates a subpool path option. • The global 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 sub-pool keyword. • 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. • The lockdown keyword disables reoptimization of the LSP.
Step 6	end Example: Router(config-if)# end	(Optional) Exits to privileged EXEC mode.

Verifying that 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:

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:

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:

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:

**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 **mplstraffic-engreoptimize** 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 {namepath-name | path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool | global] kbps] [lockdown]*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface tunnel 1	Configures an interface type and enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	tunnel destination <i>{hostname ip-address}</i> Example: 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"> • The <i>hostname</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	tunnel mpls traffic-eng path-option <i>number {dynamic explicit {namepath-name path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool global] kbps] [lockdown]</i> Example: Router(config-if)# tunnel mpls	Adds a Path Option for Bandwidth Override to specify a bandwidth fallback for a path option for an MPLS TE tunnel. <ul style="list-style-type: none"> • The <i>number</i> argument identifies the path option. • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path.

	Command or Action	Purpose
	<pre>traffic-eng path-option 1 dynamic bandwidth 500</pre>	<ul style="list-style-type: none"> The namepath-name keyword argument combination identifies the name of the explicit path option. The path-number argument identifies the number of the explicit path option. The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. The bandwidth keyword specifies LSP bandwidth. The sub-pool keyword indicates a subpool path option. The global 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 sub-pool keyword. The kbps argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. The lockdown keyword disables reoptimization of the LSP.
Step 6	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits to privileged EXEC mode.

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 **mplstraffic-engreoptimize** 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 {namepath-name | path-number} [verbatim]} [attributesstring] [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	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: <pre>Router(config)# interface tunnel 1</pre>	Configures the interface type and enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	tunnel destination <i>{hostname ip-address}</i> Example: <pre>Router(config-if)# tunnel destination 10.10.10.12</pre>	Specifies the destination of the tunnel for this path option. <ul style="list-style-type: none"> • The <i>hostname</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	tunnel mpls traffic-eng path-option <i>number {dynamic explicit {namepath-name path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool global] kbps] [lockdown]</i> Example: <pre>Router(config-if)# tunnel mpls</pre>	Adds a Path Option for Bandwidth Override to specify a bandwidth fallback for a path option for an MPLS TE tunnel. <ul style="list-style-type: none"> • The <i>number</i> argument identifies the path option. • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path.

	Command or Action	Purpose
	<pre>traffic-eng path-option 2 dynamic bandwidth 500</pre> <p>Example:</p>	<ul style="list-style-type: none"> The namepath-name keyword argument combination identifies the name of the explicit path option. The path-number argument identifies the number of the explicit path option. The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. The bandwidth keyword specifies LSP bandwidth. The sub-pool keyword indicates a subpool path option. The global 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 sub-pool keyword. The kbps argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. The lockdown keyword disables reoptimization of the LSP.
Step 6	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits to privileged EXEC mode.
Step 7	<p>show mpls traffic-eng tunnels <i>tunnel-interface</i> [brief]</p> <p>Example:</p> <pre>Router# show mpls traffic-eng tunnels tunnell</pre>	<p>(Optional) Displays information about tunnels.</p> <ul style="list-style-type: none"> Use the showmplstraffic-engtunnels command to verify which bandwidth path option is in use by the LSP.

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 {namepath-name | path-number} [verbatim]} [attributesstring] [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	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface tunnel 1	Configures an interface type and enters interface configuration mode. • The <i>type</i> argument is the type of interface that you want to configure. • The <i>number</i> argument is the number of the tunnel interface that you want to create or configure.
Step 4	tunnel destination <i>{hostname ip-address}</i> Example: Router(config-if)# tunnel destination 10.10.10.12	Specifies the destination of the tunnel for this path option. • The <i>hostname</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP address of the host destination expressed in decimal in four-part, dotted notation.
Step 5	no tunnel mpls traffic-eng path-option <i>number {dynamic explicit {namepath-name path-number} [verbatim]} [attributesstring] [bandwidth [sub-pool global] kbps] [lockdown]</i> Example: Router(config-if)# no tunnel mpls	Removes a Path Option for Bandwidth Override that specifies a bandwidth fallback for a path option for an MPLS TE tunnel. • The <i>number</i> argument identifies the path option. • The dynamic keyword indicates that the path option is dynamically calculated (the router figures out the best path). • The explicit keyword indicates that the path option is specified. You specify the IP addresses of the path.

	Command or Action	Purpose
	<pre>traffic-eng path-option 2 dynamic bandwidth 500</pre>	<ul style="list-style-type: none"> • The namepath-name keyword argument combination identifies the name of the explicit path option. • The path-number argument identifies the number of the explicit path option. • The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> • The attributesstring keyword argument combination names an attribute list to specify path options for the LSP. • The bandwidth keyword specifies LSP bandwidth. • The sub-pool keyword indicates a subpool path option. • The global 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 sub-pool keyword. • The kbps argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. • The lockdown keyword disables reoptimization of the LSP.
Step 6	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	(Optional) Exits to privileged EXEC mode.
Step 7	<p>show mpls traffic-eng tunnels <i>tunnel-interface</i> [brief]</p> <p>Example:</p> <pre>Router# show mpls traffic-eng tunnels tunnell</pre>	<p>(Optional) Displays information about tunnels.</p> <ul style="list-style-type: none"> • Use the showmplstraffic-engtunnels command to verify which bandwidth path option is in use by the LSP.

Verifying that LSP Is Signaled Using 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:

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:

Example:

```
Router# show mpls traffic-eng tunnels tunnel21
Name: Router-15-c_t21 (Tunnel21) 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 **showmplstraffic-engtunnel** 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:

Example:

```
Router# exit
Router>
```

Troubleshooting Tips

If the tunnel state is down and you configured a path-option with bandwidth override enabled, the **showmplstraffic-engtunnels** 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

This section contains the following examples for configuring LSP attribute lists:

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 and 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 `tunnelmplstraffic-engpath-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

Related Documents

Related Topic	Document Title
MPLS TE automatic bandwidth adjustment for TE tunnels configuration tasks	MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels
MPLS TE command descriptions	<i>Cisco IOS Multiprotocol Label Switching Command Reference</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
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: http://www.cisco.com/go/mibs

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>	http://www.cisco.com/techsupport

Feature Information for MPLS Traffic Engineering LSP Attributes

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 4: Feature Information for MPLS Traffic Engineering LSP Attributes

Feature Name	Releases	Feature Information
MPLS Traffic Engineering LSP Attributes	12.0(26)S 12.2(33)SRA 12.2(33)SXH 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>The following commands were introduced or modified: affinity (LSP Attributes), auto-bw (LSP Attributes), bandwidth (LSP Attributes), exit(LSP Attributes), list(LSP Attributes), lockdown(LSP Attributes), mplstraffic-englspattributes, priority(LSP Attributes), protection(LSP Attributes), record-route(LSP Attributes), showmplstraffic-englspattributes, and showmplstraffic-engltunnels.</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.



MPLS Traffic Engineering AutoTunnel Mesh Groups

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) devices.

- [Finding Feature Information, page 103](#)
- [Prerequisites for MPLS Traffic Engineering--AutoTunnel Mesh Groups, page 104](#)
- [Restrictions for MPLS Traffic Engineering--AutoTunnel Mesh Groups, page 104](#)
- [Information About MPLS Traffic Engineering--AutoTunnel Mesh Groups, page 104](#)
- [How to Configure MPLS Traffic Engineering--AutoTunnel Mesh Groups, page 106](#)
- [Configuration Examples for MPLS Traffic Engineering--Autotunnel Mesh Groups, page 116](#)
- [Additional References, page 118](#)
- [Feature Information for MPLS Traffic Engineering--Autotunnel Mesh Groups, page 118](#)
- [Glossary, page 120](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering--AutoTunnel Mesh Groups

- Be knowledgeable about MPLS TE. See the [Additional References](#), on page 118.
- 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

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 device has a tunnel to each of the other PE devices.
- 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 devices.

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 devices), 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 device is added to the network.
- Enable existing devices to configure TE LSPs to new PE devices.
- Enable the construction of a mesh of TE LSPs among the PE devices 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 devices 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 device 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 device 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](#), on page 115.

OSPF can advertise mesh group IDs for an OSPF area. OSPF is the only IGP supported in some software releases of the MPLS Traffic Engineering--Autotunnel Mesh Groups feature.

How to Configure MPLS Traffic Engineering--AutoTunnel Mesh Groups

Configuring a Mesh of TE Tunnel LSPs

Perform the following tasks on each PE device in your network to configure a mesh of TE tunnel LSPs:



Note

You can perform these tasks in any order.

Enabling Autotunnel Mesh Groups Globally

Perform this task on all PE devices 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	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	mpls traffic-eng auto-tunnel mesh Example: Device(config)# mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.

	Command or Action	Purpose
Step 4	end Example: Device(config)# end	Exits to privileged EXEC mode.

Creating 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 devices 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	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	ip access-list { standard extended } <i>access-list-name</i> Example: Device(config)# ip access-list standard a1	Defines an IP access list using a name and enters standard named access list configuration mode. <ul style="list-style-type: none"> • The standard keyword specifies a standard IP access list. • The extended keyword specifies an extended IP access list. • 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.

	Command or Action	Purpose
Step 4	<p><code>permit source [source-wildcard]</code></p> <p>Example:</p> <pre>Device(config-std-nacl)# permit 10.0.0.0 0.255.255.255</pre>	<p>Sets conditions to allow a packet to pass a named IP access list.</p> <ul style="list-style-type: none"> 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"> Use a 32-bit quantity in four-part dotted decimal format. Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0. 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"> Use a 32-bit quantity in four-part dotted decimal format. Place 1s in the bit positions you want to ignore. Use the any keyword as an abbreviation for a source and source-wildcard of 0.0.0.0 255.255.255.255. Use host source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
Step 5	<p><code>end</code></p> <p>Example:</p> <pre>Device(config-std-nacl)# end</pre>	Exits to privileged EXEC mode.

Creating an Autotunnel Template Interface

Creating an autotunnel template interface helps minimize the initial configuration of the network. You configure one template interface per mesh, which 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 path-option** *number* {dynamic | explicit {name *path-name* | *path-number*}}
[lockdown]
9. **tunnel destination access-list** *num*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface auto-template <i>interface-num</i> Example: Device(config)# interface auto-template 1	Creates a template interface and enters interface configuration mode. • The <i>interface-num</i> argument is the interface number. Valid values are from 1 to 25.
Step 4	ip unnumbered <i>interface-type</i> <i>interface-number</i> Example: Device(config-if)# ip unnumbered Loopback 0	Enables IP processing on an interface without assigning an explicit IP address to the interface. • The <i>type</i> and <i>number</i> arguments name the type and number of another interface on which the device has an assigned IP address. It cannot be another unnumbered interface.
Step 5	tunnel mode {aurp cayman dvmrp eon gre ipip iptalk mpls nos}	Sets the encapsulation mode for the tunnel interface.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device(config-if)# tunnel mode mpls</pre>	
Step 6	<p>tunnel mpls traffic-eng autoroute announce</p> <p>Example:</p> <pre>Device(config-if)# tunnel mpls traffic-eng autoroute announce</pre>	Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first algorithm (SPF) calculation.
Step 7	<p>tunnel mpls traffic-eng priority <i>setup-priority [hold-priority]</i></p> <p>Example:</p> <pre>Device(config-if)# tunnel mpls traffic-eng priority 1 1</pre>	<p>Configures the setup and reservation priority for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> 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. 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.
Step 8	<p>tunnel mpls traffic-eng path-option <i>number</i> {dynamic explicit {name <i>path-name</i> <i>path-number</i>}} [lockdown]</p> <p>Example:</p> <pre>Device(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"> The <i>number</i> argument is the number of the path option. When multiple path options are configured, lower numbered options are preferred. The dynamic keyword specifies that the path of the LSP is dynamically calculated. The explicit keyword specifies that the path of the LSP is an IP explicit path. The name <i>path-name</i> keyword-argument pair is the path name of the IP explicit path that the tunnel uses with this option. The <i>path-number</i> argument is the path number of the IP explicit path that the tunnel uses with this option. The lockdown keyword specifies that the LSP cannot be reoptimized.
Step 9	<p>tunnel destination access-list <i>num</i></p> <p>Example:</p> <pre>Device(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"> The <i>num</i> argument is the number of the access list.

	Command or Action	Purpose
Step 10	end Example: Device(config)# end	Exits to privileged EXEC mode.

Specifying 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	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	mpls traffic-eng auto-tunnel mesh tunnel-num min <i>num</i> max <i>num</i> Example: Device(config)# mpls traffic-eng auto-tunnel mesh tunnel-num min 1000 max 2000	Specifies the range of mesh tunnel interface numbers. <ul style="list-style-type: none"> • The min <i>num</i> keyword-argument pair specifies the beginning number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535. • The max <i>num</i> keyword-argument pair specifies the ending number of the range of mesh tunnel interface numbers. Valid values are from 1 to 65535.

	Command or Action	Purpose
Step 4	end Example: Device(config)# end	Exits to privileged EXEC mode.

Displaying Configuration Information About Tunnels

SUMMARY STEPS

1. **enable**
2. **show running interface auto-template *num***
3. **show interface tunnel *num* configuration**
4. **exit**

DETAILED STEPS

Step 1 **enable**
 Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

Example:

```
Device> enable
Device#
```

Step 2 **show running interface auto-template *num***
 Use this command to display interface configuration information for a tunnel interface. For example:

Example:

```
Device# show running interface auto-template 1
interface auto-templatel
 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-templatel 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:

Example:

```
Device# 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:

Example:

```
Device# exit
Device>
```

Monitoring 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:

Example:

```
Device> enable
Device#
```

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:

Example:

```
Device# 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
device_t64336                   10.2.2.2       -          Se2/0
up/up
device_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:

Example:

```

Device# 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:

Example:

```

Device# exit
Device>

```

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	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	mpls traffic-eng auto-tunnel mesh Example: Device(config)# mpls traffic-eng auto-tunnel mesh	Enables autotunnel mesh groups globally.
Step 4	router ospf <i>process-id</i> Example: Device(config)# router ospf 100	Enters router configuration mode and configures an OSPF routing process. <ul style="list-style-type: none"> • 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.

	Command or Action	Purpose
Step 5	<p>mpls traffic-eng mesh-group <i>mesh-group-id</i> <i>interface-type interface-number area area-id</i></p> <p>Example:</p> <pre>Device(config-router)# mpls traffic-eng mesh-group 10 loopback 0 area 100</pre>	<p>Advertises the autotunnel mesh group number of an LSR.</p> <ul style="list-style-type: none"> • The <i>mesh-group-id</i> is a number that identifies a specific mesh group. • The <i>interface-type</i> and <i>interface-number</i> arguments specify a type of interface and an interface number. • The area <i>area-id</i> keyword-argument pair identifies the area.
Step 6	<p>exit</p> <p>Example:</p> <pre>Device(config-router)# exit</pre>	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	<p>interface auto-template <i>interface-num</i></p> <p>Example:</p> <pre>Device(config)# interface auto-template 1</pre>	<p>Creates a template interface and enters interface configuration mode.</p> <ul style="list-style-type: none"> • The <i>interface-num</i> argument identifies the interface number. Valid values are from 1 to 25.
Step 9	<p>tunnel destination mesh-group <i>mesh-group-id</i></p> <p>Example:</p> <pre>Device(config-if)# tunnel destination mesh-group 10</pre>	<p>Specifies a mesh group that a template interface uses to signal tunnels for all mesh group members.</p> <ul style="list-style-type: none"> • The <i>mesh-group-id</i> is a number that identifies a specific mesh group.
Step 10	<p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre>	Exits to privileged EXEC mode.

Configuration Examples for MPLS Traffic Engineering--Autotunnel Mesh Groups

Examples: Configuring a Mesh of TE Tunnel LSPs

This section contains the following configuration examples for configuring a mesh of TE tunnel LSP:

Example: Enabling Autotunnel Mesh Groups Globally

The following example shows how to enable autotunnel mesh groups globally:

```
configure terminal
!
mpls traffic-eng auto-tunnel mesh
end
```

Example: Creating an Access List Using a Name

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.

Example: Creating an AutoTunnel Template Interface

This example shows how to create an AutoTunnel 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 path-option 1 dynamic
 tunnel destination access-list a1
end
```

Example: Specifying the Range of Mesh Tunnel Interface Numbers

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
```

Example: Configuring IGP Flooding for Autotunnel Mesh Groups

In the following example, OSPF is configured to advertise the device 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

Related Documents

Related Topic	Document Title
MPLS traffic engineering command descriptions	<i>Multiprotocol Label Switching Command Reference</i>

Technical Assistance

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

Feature Information for MPLS Traffic Engineering--Autotunnel Mesh Groups

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 5: Feature Information for MPLS Traffic Engineering--Autotunnel Mesh Groups

Feature Name	Releases	Feature Information
MPLS Traffic Engineering--Autotunnel Mesh Groups	12.0(27)S 12.0(29)S 12.2(33)SRA 12.2(33)SXH 12.4(20)T 12.2(33)SRE Cisco IOS XE Release 3.6S	<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 device with autotunnel mesh groups can be configured with stateful switchover (SSO) redundancy.</p> <p>In Cisco IOS XE Release 3.6S, this feature was integrated.</p> <p>These commands were introduced or modified: mpls traffic-eng auto-tunnel mesh, mpls traffic-eng auto-tunnel mesh tunnel-num, mpls traffic-eng mesh-group, show mpls traffic-eng auto-tunnel mesh.</p>

Feature Name	Releases	Feature Information
MPLS TE--Autotunnel/Auotmesh SSO Coexistence	Cisco IOS XE Release 3.5S 15.0(1)S	In Cisco IOS XE Release 3.5S, this feature was integrated. In Cisco IOS Release 15.0(1)S, this feature was integrated. Note Starting with Cisco IOS Release 15.2(2)S and Cisco IOS XE Release 3.6S, the SSO Support for MPLS TE Autotunnel and Automesh feature replaces the MPLS TE - Autotunnel/Automesh SSO Coexistence feature. For more information, see the <i>MPLS High Availability Configuration Guide</i> for the new implementation.

Glossary

CE device --customer edge device. A device that is part of a customer's network and interfaces to a provider edge (PE) device.

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 device --A device 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 devices 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 device that forwards a packet based on the value of a label encapsulated in the packet.

mesh group --A set of label switch devices (LSRs) that are members of a full or partial network of traffic engineering (TE) label switched paths (LSPs).

P device --provider core device.

PE device --provider edge device. A device at the edge of the service provider's network that interfaces to customer edge (CE) devices.

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 devices. 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.



CHAPTER 6

MPLS Traffic Engineering Verbatim Path Support

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, page 123](#)
- [Prerequisites for MPLS Traffic Engineering--Verbatim Path Support, page 124](#)
- [Restrictions for MPLS Traffic Engineering--Verbatim Path Support, page 124](#)
- [Information About MPLS Traffic Engineering--Verbatim Path Support, page 124](#)
- [How to Configure MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels, page 125](#)
- [Configuration Examples for MPLS Traffic Engineering Verbatim Path Support, page 128](#)
- [Additional References, page 129](#)
- [Feature Information for MPLS Traffic Engineering Verbatim Path Support, page 130](#)
- [Glossary, page 131](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering--Verbatim Path Support

- A Multiprotocol Label Switching (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 MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels

Configuring 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 }}`
11. `exit`
12. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
Step 3	<p><code>interface tunnel number</code></p> <p>Example:</p> <pre>Router(config)# interface tunnel 1</pre>	<p>Configures a tunnel interface and enters interface configuration mode.</p> <ul style="list-style-type: none"> • The <i>number</i> argument identifies the tunnel number to be configured.

	Command or Action	Purpose
Step 4	<p>ip unnumbered loopback <i>number</i></p> <p>Example:</p> <pre>Router(config-if) # ip unnumbered loopback 1</pre>	<p>Configures an unnumbered IP interface, which enables IP processing without an explicit address. A loopback interface is usually configured with the router ID.</p> <p>Note An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.</p>
Step 5	<p>tunnel destination <i>{host-name ip-address}</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel destination 10.100.100.100</pre>	<p>Specifies the destination for a tunnel.</p> <ul style="list-style-type: none"> • The <i>host-name</i> argument is the name of the host destination. • The <i>ip-address</i> argument is the IP Version 4 address of the host destination expressed in decimal in four-part, dotted notation.
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	<p>Sets the tunnel encapsulation mode to MPLS traffic engineering.</p>
Step 7	<p>tunnel mpls traffic-eng bandwidth <i>{sub-pool kbps kbps}</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 1000</pre>	<p>Configures the bandwidth required for an MPLS TE tunnel and assigns it either to the sub-pool or the global pool.</p> <ul style="list-style-type: none"> • The sub-pool keyword indicates a subpool tunnel. • 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.
Step 8	<p>tunnel mpls traffic-eng autoroute announce</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng autoroute announce</pre>	<p>Specifies that IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.</p>
Step 9	<p>tunnel mpls traffic-eng priority <i>setup-priority [hold-priority]</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng priority 1 1</pre>	<p>Configures setup and reservation priority for a tunnel.</p> <ul style="list-style-type: none"> • 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. <p>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.</p> <ul style="list-style-type: none"> • 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. <p>Valid values are from 0 to 7, where a lower number indicates a higher priority.</p>

	Command or Action	Purpose
Step 10	<p>tunnel mpls traffic-eng path-option <i>preference-number</i> {dynamic [attributes <i>string</i> bandwidth {sub-pool <i>kbps</i> <i>kbps</i>} lockdown verbatim] explicit{name <i>path-name</i> identifier <i>path-number</i> }}</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test verbatim</pre> <p>Example:</p>	<p>Specifies LSP-related parameters, including the verbatim keyword used with an explicit path option, for an MPLS TE tunnel.</p> <ul style="list-style-type: none"> • The <i>preference-number</i> argument identifies the path option. • The protect keyword and <i>preference-number</i> argument identify the path option with protection. • The dynamic keyword indicates that the path option is dynamically calculated. (The router figures out the best path.) • The explicit keyword indicates that the path option is specified. The IP addresses are specified for the path. • The name <i>path-name</i> keyword argument combination identifies the name of the explicit path option. • The <i>path-number</i> argument identifies the number of the explicit path option. • The verbatim keyword bypasses the topology database verification. <p>Note You can use the verbatim keyword only with the explicit path option.</p> <ul style="list-style-type: none"> • The attributes <i>string</i> keyword argument combination names an attribute list to specify path options for the LSP. • The bandwidth keyword specifies the LSP bandwidth. • The sub-pool keyword indicates a subpool path option. • 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. • The lockdown keyword disables reoptimization of the LSP.
Step 11	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	<p>Exits interface configuration mode and returns to global configuration mode.</p>
Step 12	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

Verifying Verbatim 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	<p><code>enable</code></p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>show mpls traffic-eng tunnels tunnel-interface [brief]</code></p> <p>Example:</p> <pre>Router# show mpls traffic-eng tunnels tunnel1</pre>	<p>Displays information about tunnels including those configured with an explicit path option using verbatim.</p>
Step 3	<p><code>disable</code></p> <p>Example:</p> <pre>Router# disable</pre>	<p>(Optional) Exits to user EXEC mode.</p>

Configuration Examples for MPLS Traffic Engineering Verbatim Path Support

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

Related Documents

Related Topic	Document Title
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP) feature module

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

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>	<p>http://www.cisco.com/techsupport</p>

Feature Information for MPLS Traffic Engineering Verbatim Path Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 6: Feature Information for MPLS Traffic Engineering Verbatim Path Support

Feature Name	Releases	Feature Information
MPLS Traffic Engineering: Verbatim Path Support	12.0(26)S 12.2(33)SRA 12.2(33)SXH 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>The following commands were introduced or modified: show mpls traffic-eng tunnels, tunnel mpls traffic-eng path option.</p>

Glossary

Fast Reroute --Procedures that enable temporary routing around a failed link or node while a new label-switched path (LSP) is being established at the head end.

headend --The router that originates and maintains a given label-switched path (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 Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information protocol (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 Multiprotocol Label Switching (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 label-switched path (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.



MPLS Traffic Engineering RSVP Hello State Timer

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, page 133](#)
- [Prerequisites for MPLS Traffic Engineering--RSVP Hello State Timer, page 134](#)
- [Restrictions for MPLS Traffic Engineering--RSVP Hello State Timer, page 134](#)
- [Information About MPLS Traffic Engineering - Configurable Path Calculation Metric for Tunnels, page 134](#)
- [How to Configure MPLS Traffic Engineering--RSVP Hello State Timer, page 137](#)
- [Configuration Examples for MPLS Traffic Engineering--RSVP Hello State Timer, page 143](#)
- [Additional References, page 143](#)
- [Command Reference, page 145](#)
- [Feature Information for MPLS Traffic Engineering--RSVP Hello State Timer, page 145](#)
- [Glossary, page 146](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

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 - Configurable Path Calculation Metric for Tunnels

Hellos for State Timeout

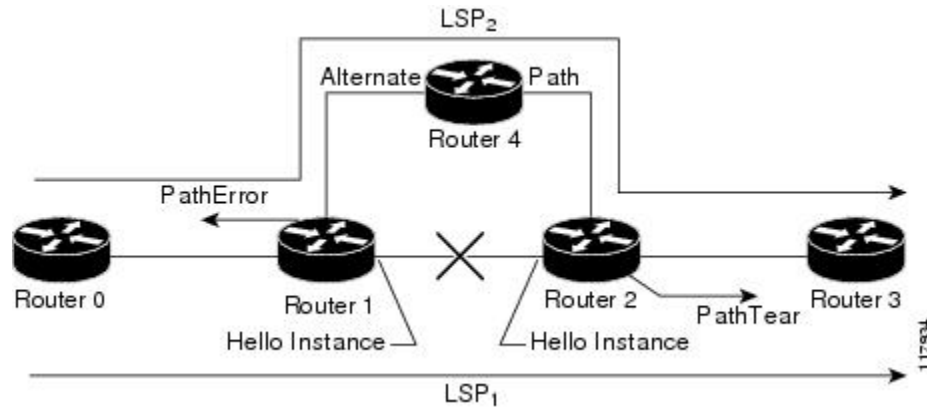
When RSVP signals a TE LSP and there is a failure somewhere along the path, the failure can remain undetected for as long as two minutes. During this time, bandwidth is held by the nonfunctioning LSP on the nodes downstream from the point of failure along the path with the state intact. If this bandwidth 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

The figure below shows a nonfast-reroutable TE LSP from Router 1 to Router 3 via Router 2.



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.

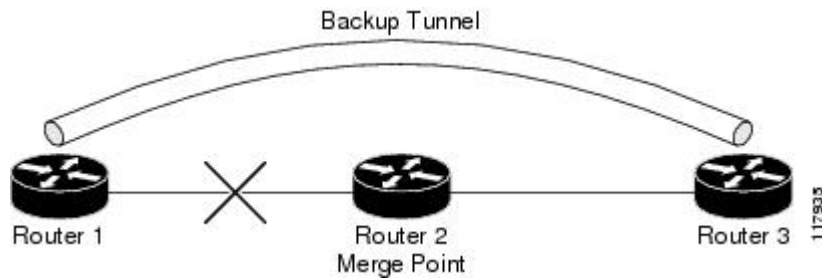
LSP1 goes from Router 0 to Router 1 to Router 2 to Router 3; LSP 2 goes from Router 0 to Router 1 to Router 4 to Router 2 to Router 3.

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

The figure below shows a fast reroutable TE LSP with a backup tunnel from Router1 to Router 2 to Router 3.



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.

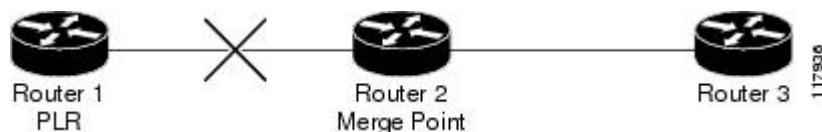
Fast-Reroutable TE LSP Without Backup Tunnel

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.

The figure below 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.



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

**Note**

The following tasks also enable Fast Reroute; however, this section focuses on the RSVP hello state timer.

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip rsvp signalling hello Example: Router(config)# ip rsvp signalling hello	Enables hellos for state timeout globally on a router.

	Command or Action	Purpose
Step 4	end Example: Router(config)# end	Exits to privileged EXEC mode.

Enabling the 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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet 0/0	Enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type number</i> arguments identify the interface to be configured.
Step 4	ip rsvp signalling hello Example: Router(config-if)# ip rsvp signalling hello	Enables hellos for state timeout on an interface.

	Command or Action	Purpose
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Setting a DSCP Value 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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet 0/0	Enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type number</i> arguments identify the interface to be configured.
Step 4	ip rsvp signalling hello reroute dscp <i>num</i> Example: 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.

	Command or Action	Purpose
Step 5	end Example: Router(config-if)# end	Exits to privileged EXEC mode.

Setting 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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> Example: Router(config)# interface Ethernet 0/0	Enters interface configuration mode. <ul style="list-style-type: none"> • The <i>type number</i> argument identifies the interface to be configured.

	Command or Action	Purpose
Step 4	<p>ip rsvp signalling hello reroute refresh interval <i>interval-value</i></p> <p>Example:</p> <pre>Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000</pre>	Sets a hello request interval on an interface of a router with hellos for state timer enabled.
Step 5	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	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	<p>enable</p> <p>Example:</p> <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface <i>type number</i></p>	Enters interface configuration mode.

	Command or Action	Purpose
	Example: <pre>Router(config)# interface Ethernet 0/0</pre>	<ul style="list-style-type: none"> The <i>type number</i> arguments identify the interface to be configured.
Step 4	ip rsvp signalling hello reroute refresh misses <i>msg-count</i> Example: <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	end Example: <pre>Router(config-if)# end</pre>	Exits to privileged EXEC mode.

Verifying Hello for State Timer Configuration

SUMMARY STEPS

1. enable
2. show ip rsvp hello

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: <pre>Router> enable</pre>	(Optional) Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show ip rsvp hello Example: <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

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

Related Documents

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
QoS features including signaling, classification, and congestion management	<i>Cisco IOS Quality of Service Solutions Configuration Guide</i>
Stateful Switchover	<i>Cisco IOS High Availability Configuration Guide</i>
MPLS Label Distribution Protocol	MPLS Label Distribution Protocol (LDP) Overview
Cisco nonstop forwarding	Cisco Nonstop Forwarding
Information on backup tunnels, link and node failures, RSVP hellos	MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
Graceful restart	NSF/SSO - MPLS TE and RSVP Graceful Restart

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

RFCs

RFC	Title
RFC 3209	RSVP-TE: Extensions to RSVP for LSP Tunnels

Technical Assistance

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

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Multiprotocol Label Switching Command Reference* at http://www.cisco.com/en/US/docs/ios/mpls/command/reference/mp_book.html. For information about all Cisco IOS commands, 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.

- **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

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 7: 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 12.2(33)SRA 12.2(33)SXH 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.

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

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, page 149](#)
- [Prerequisites for MPLS Traffic Engineering Forwarding Adjacency, page 150](#)
- [Restrictions for MPLS Traffic Engineering Forwarding Adjacency, page 150](#)
- [Information About MPLS Traffic Engineering Forwarding Adjacency, page 150](#)
- [How to Configure MPLS Traffic Engineering Forwarding Adjacency, page 151](#)
- [Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency, page 155](#)
- [Additional References, page 157](#)
- [Glossary, page 158](#)
- [Feature Information for MPLS Traffic Engineering Forwarding Adjacency, page 159](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering Forwarding Adjacency

Your network must support the following Cisco IOS XE features:

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

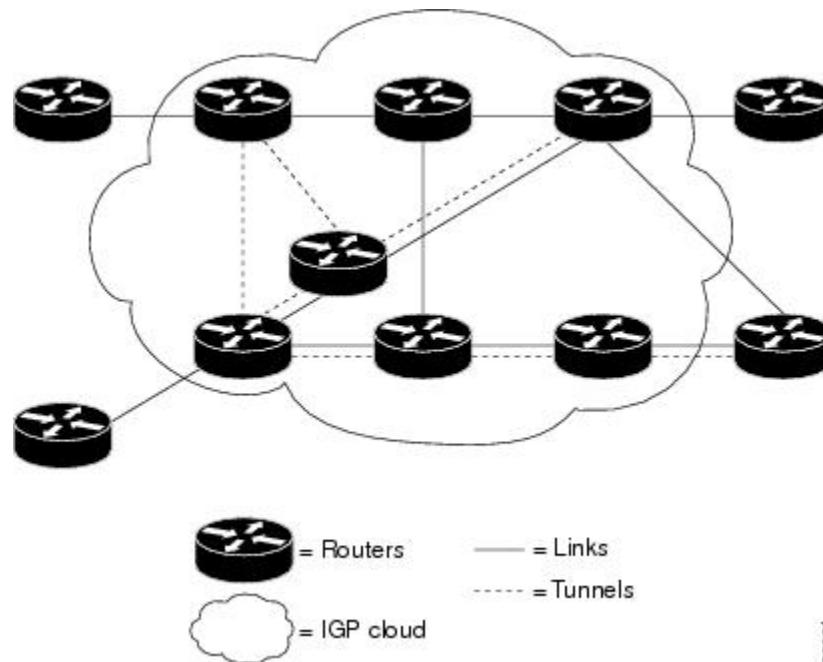
Restrictions for MPLS Traffic Engineering Forwarding Adjacency

- 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.

Information About MPLS Traffic Engineering Forwarding Adjacency

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 the figure below.



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 IGPs to compute the SPF even if they are not the headend of any TE tunnels.

How to Configure MPLS Traffic Engineering Forwarding Adjacency

Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **exit**
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 0	Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode.
Step 4	exit Example: Router(config-if)# exit	Exits interface configuration mode and returns to global configuration mode.
Step 5	exit Example: Router(config)# exit	Exits global configuration mode and returns to privileged EXEC mode.

Configuring MPLS TE Forwarding Adjacency on Tunnels

**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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 0	Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode.
Step 4	tunnel mpls traffic-eng forwarding-adjacency [<i>holdtime value</i>] Example: Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency	Advertises a TE tunnel as a link in an IGP network.
Step 5	isis metric {<i>metric-value</i> maximum} {<i>level-1</i> level-2} Example: 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"> • You should specify the isis metric 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.

Verifying MPLS TE Forwarding Adjacency

SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng forwarding-adjacency** [*ip-address*]
3. **show isis** [*process-tag*] **database** [*level-1*] [*level-2*] [*I1*] [*I2*] [*detail*] [*lspid*]
4. **exit**

DETAILED STEPS

Step 1 enable

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

Example:

```
Router> enable
Router#
```

Step 2 show mpls traffic-eng forwarding-adjacency [*ip-address*]

Use this command to see the current tunnels. For example:

Example:

```
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 3 show isis [*process-tag*] database [*level-1*] [*level-2*] [*I1*] [*I2*] [*detail*] [*lspid*]

Use this command to display information about the IS-IS link-state database. For example:

Example:

```
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
```

Step 4**exit**

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

Example:

```
Router# exit
Router>
```

Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency

This section provides a configuration example for the MPLS Traffic Engineering Forwarding Adjacency feature using an IS-IS metric.

Example MPLS TE Forwarding Adjacency

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 ODPF:

```
Router# configure terminal
```

```

Router# show running-config

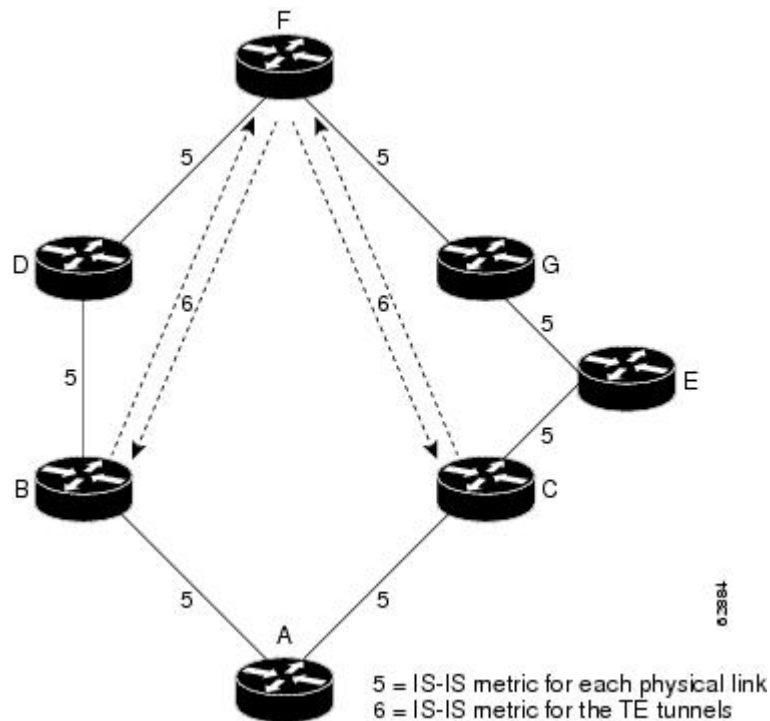
Building configuration...
Current configuration : 310 bytes
interface tunnel 1
!
interface Tunnell
 ip unnumbered Loopback0
 ip ospf cost 6
 tunnel destination 172.16.255.5
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency tunnel mpls
 traffic-eng priority 7 7
 tunnel mpls traffic-eng 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 the figure below, 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.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MPLS traffic engineering commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>
IP switching commands	<i>Cisco IOS IP Switching Command Reference</i>
IS-IS TLVs	Intermediate System-to-Intermediate System (IS-IS) TLVs (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 software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

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 IGP 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.

Feature Information for MPLS Traffic Engineering Forwarding Adjacency

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 8: Feature Information for MPLS Traffic Engineering Forwarding Adjacency

Feature Name	Releases	Feature Information
MPLS Traffic Engineering Forwarding Adjacency	12.0(15)S 12.0(16)ST 12.2(18)S 12.2(18)SXD 12.2(27)SBC 12.2(28)SB 12.4(20)T Cisco IOS XE Release 2.3	<p>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.</p> <p>In 12.0(15)S, this feature was introduced.</p> <p>In 12.0(16)ST, this feature was integrated.</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 12.4(20)T, this feature was integrated.</p> <p>In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.</p> <p>The following commands were modified: debug mpls traffic-eng forwarding-adjacency, show mpls traffic-eng forwarding-adjacency, and tunnel mpls traffic-eng forwarding-adjacency.</p>



MPLS Traffic Engineering Interarea Tunnels

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, page 161](#)
- [Prerequisites for MPLS Traffic Engineering Interarea Tunnels, page 162](#)
- [Restrictions for MPLS Traffic Engineering Interarea Tunnels, page 162](#)
- [Information About MPLS Traffic Engineering Interarea Tunnels, page 162](#)
- [How to Configure MPLS Traffic Engineering Interarea Tunnels, page 165](#)
- [Configuration Examples for MPLS Traffic Engineering Interarea Tunnels, page 180](#)
- [Additional References, page 185](#)
- [Feature Information for MPLS Traffic Engineering Interarea Tunnels, page 186](#)
- [Glossary, page 187](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering Interarea Tunnels

Your network must support the following software 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.
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

Information About MPLS Traffic Engineering Interarea Tunnels

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.

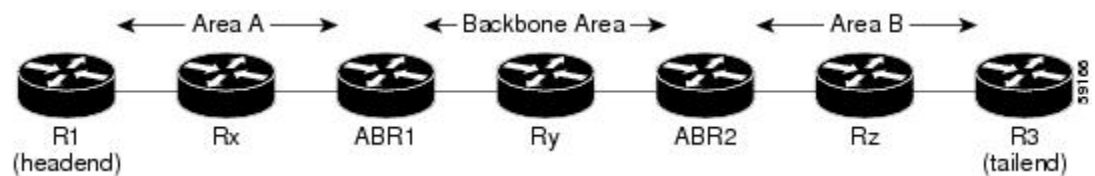
For example, to configure a TE tunnel from router R1 to router R3 in the simple multiarea network shown in the figure below, you would specify ABR1 and ABR2 as loose hops in the explicit path for the tunnel.



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 5: 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

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



Note You must configure either OSPF or IS-IS.

Configuring OSPF for Interarea Tunnels

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.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>router ospf process-id</p> <p>Example:</p> <pre>Router(config)# router ospf 1</pre>	<p>Enables OSPF and enters router configuration mode.</p> <p>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.</p>
Step 4	<p>network ip-address wildcard-mask area area-id</p> <p>Example:</p> <pre>Router(config-router)# network 192.168.45.0 0.0.255.255 area 1</pre>	Specifies the interfaces on which OSPF is to run and specifies the area to which the interface is connected.
Step 5	<p>mpls traffic-eng router-id interface-name</p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng router-id Loopback0</pre>	<p>Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.</p> <p>The router identifier is displayed in the show mpls traffic-eng topology path command output.</p> <p>Note The <i>interface-name</i> value must be Loopback0.</p>
Step 6	<p>mpls traffic-eng area 0</p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng area 0</pre>	<p>Turns on MPLS traffic engineering for OSPF in area 0.</p> <p>Note To display the MPLS TE global topology currently known at this node, use the show mpls traffic-eng topology command.</p>
Step 7	<p>mpls traffic-eng area number</p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng area 2</pre>	Configures a router running OSPF MPLS to flood traffic engineering for the indicated OSPF area.
Step 8	<p>end</p> <p>Example:</p> <pre>Router(config-router)# end</pre>	Returns to privileged EXEC mode.

Configuring OSPF for Non-ABR Routers

For each non-ABR that is running OSPF, perform the following steps to configure OSPF.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router ospf <i>process-id</i> Example: Router(config)# router ospf 1	Enables OSPF and enters router configuration mode. 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	<p>network <i>ip-address wildcard-mask area area-id</i></p> <p>Example:</p> <pre>Router(config-router)# network 192.168.10.10 255.255.255.0 area 1</pre>	Specifies the interfaces on which OSPF is to run and specifies the area to which the interface is connected.
Step 5	<p>mpls traffic-eng router-id <i>interface-name</i></p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng router-id Loopback0</pre>	<p>Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.</p> <p>The router identifier is displayed in the show mpls traffic-eng topology path command output.</p> <p>Note The <i>interface-name</i> value must be Loopback0.</p>
Step 6	<p>mpls traffic-eng area <i>number</i></p> <p>Example:</p> <pre>Router(config-router)# mpls traffic-eng area 1</pre>	<p>Specifies the area that the router is in.</p> <p>Note To display the MPLS TE global topology currently known at this node, use the show mpls traffic-eng topology command.</p>
Step 7	<p>end</p> <p>Example:</p> <pre>Router(config-router)# end</pre>	Returns to privileged EXEC mode.

Configuring IS-IS for Interarea Tunnels

Configuring IS-IS for Backbone Routers

To configure IS-IS for background (level-1-2) routers, perform the following steps.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **net *nn.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	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router isis Example: 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	metric-style wide Example: Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style type, length, value objects (TLVs).
Step 5	net <i>nn.nnnn.nnnn.nnnn</i> Example: Router(config-router)# net 10.0000.0100.0000.0010	Configures the area ID (area address) and the system ID.

	Command or Action	Purpose
Step 6	mpls traffic-eng router-id <i>interface-name</i> Example: <pre>Router(config-router)# mpls traffic-eng router-id Loopback0</pre>	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0.
Step 7	mpls traffic-eng level-1 Example: <pre>Router(config-router)# mpls traffic-eng level-1</pre>	Turns on MPLS traffic engineering for IS-IS at level 1. Note To display the MPLS TE global topology currently known at this node, use the show mpls traffic-eng topology command.
Step 8	mpls traffic-eng level-2 Example: <pre>Router(config-router)# mpls traffic-eng level-2</pre>	Turns on MPLS traffic engineering for IS-IS at level 2. Note To display the MPLS TE global topology currently known at this node, use the show mpls traffic-eng topology command.
Step 9	interface <i>typeslot / port</i> Example: <pre>Router(config-router)# interface POS1/0</pre>	Configures an interface type and enters interface configuration mode.
Step 10	ip router isis Example: <pre>Router(config-if)# ip router isis</pre>	Enables IS-IS routing. Specify this command on each interface on which you want to run IS-IS.
Step 11	end Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Configuring IS-IS for Nonbackbone Routers

To configure IS-IS for nonbackbone routers, perform the following steps.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router isis Example: 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	metric-style wide Example: Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style TLVs.
Step 5	net <i>nn.nnnn.nnnn.nnnn.nnnn</i> Example: Router(config-router)# net 10.0000.2000.0100.0001	Configures the area ID (area address) and the system ID.
Step 6	mpls traffic-eng router-id <i>interface-name</i> Example: Router(config-router)# mpls traffic-eng router-id Loopback0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0.

	Command or Action	Purpose
Step 7	mpls traffic-eng {level-1 level-2} Example: <pre>Router(config-router)# mpls traffic-eng level-1</pre>	Turns on MPLS traffic engineering for IS-IS at level 1. Note To display the MPLS TE global topology currently known at this node, use the show mpls traffic-eng topology command.
Step 8	end Example: <pre>Router(config-router)# end</pre>	Returns to privileged EXEC mode.

Configuring IS-IS for Interfaces

To configure IS-IS for interfaces, perform the following steps.



Note MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis**
4. **metric-style wide**
5. **net nn.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	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

	Command or Action	Purpose
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router isis Example: 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	metric-style wide Example: Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style TLVs.
Step 5	net nn.nnnn.nnnn.nnnn Example: Router(config-router)# net 10.0000.0100.0000.0010	Configures the area ID (area address) and the system ID.
Step 6	mpls traffic-eng router-id interface-name Example: Router(config-router)# mpls traffic-eng router-id Loopback0	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface Loopback0.
Step 7	interface typeslot /port Example: Router(config-router)# interface POS1/0	Specifies the interface and enters interface configuration mode.
Step 8	ip router isis Example: Router(config-if)# ip router isis	Enables IS-IS routing. Specify this command on each interface on which you want to run IS-IS.
Step 9	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Configuring MPLS and RSVP to Support Traffic Engineering

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	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip cef Example: Router(config)# ip cef	Enables Cisco Express Forwarding on the Route Processor card.
Step 4	mpls traffic-eng tunnels Example: Router(config)# mpls traffic-eng tunnels	Enables MPLS traffic engineering tunnel signaling on a device.
Step 5	interface <i>typeslot / port</i> Example: Router(config)# interface Loopback0	Specifies the interface and enters interface configuration mode.

	Command or Action	Purpose
Step 6	ip address <i>ip-address mask</i> [secondary [<i>vrf vrf-name</i>]] Example: <pre>Router(config-if)# ip address 192.168.10.10 255.255.255.255</pre>	Assigns an IP network address and network mask to the interface.
Step 7	ip rsvp bandwidth Example: <pre>Router(config-if)# ip rsvp bandwidth</pre>	Enables RSVP for IP on an interface.
Step 8	end Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Configuring an MPLS Traffic Engineering Interarea Tunnel

Configuring an MPLS Traffic Engineering Interarea Tunnel to Use Explicit Paths

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	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface <i>tunnel-interface</i></p> <p>Example:</p> <pre>Router(config)# interface Tunell</pre>	Configures an interface type and enters interface configuration mode.
Step 4	<p>ip unnumbered <i>type number</i></p> <p>Example:</p> <pre>Router(config-if)# ip unnumbered Loopback 0</pre>	<p>Gives the tunnel interface an IP address.</p> <p>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.</p>
Step 5	<p>tunnel destination <i>ip-address</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel destination 192.168.20.20</pre>	<p>Specifies the destination for a tunnel.</p> <p>You must enter the MPLS traffic engineering router ID of the destination device.</p>
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 7	<p>tunnel mpls traffic-eng bandwidth <i>bandwidth</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 300</pre>	Configures the bandwidth required for the MPLS traffic engineering tunnel.
Step 8	<p>tunnel mpls traffic-eng path-option <i>number explicit {name <i>path-name</i> identifier <i>path-number</i>}</i> [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name path-Tunell</pre>	<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 name keyword must specify the ABRs the tunnel LSP must traverse as loose hops via the next-address loose command.</p>

	Command or Action	Purpose
Step 9	end Example: Router(config-if)# end	Returns to privileged EXEC mode.

Configuring Explicit Paths

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip explicit-path name <i>pathname</i> Example: Router(config)# ip explicit-path name path-tunnell	Enters IP explicit path configuration mode and creates or modifies the specified path.
Step 4	next-address [loose strict] <i>ip-address</i> Example: Router(config-ip-expl-path)# next-address loose 192.168.40.40	Specifies the next IP address in the explicit path. In a next-address loose command you must specify each ABR the path must traverse.

	Command or Action	Purpose
Step 5	end Example: Router(config-ip-expl-path)# end	Returns to privileged EXEC mode.

Configuring an MPLS Traffic Engineering Tunnel with Autoroute Destination

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

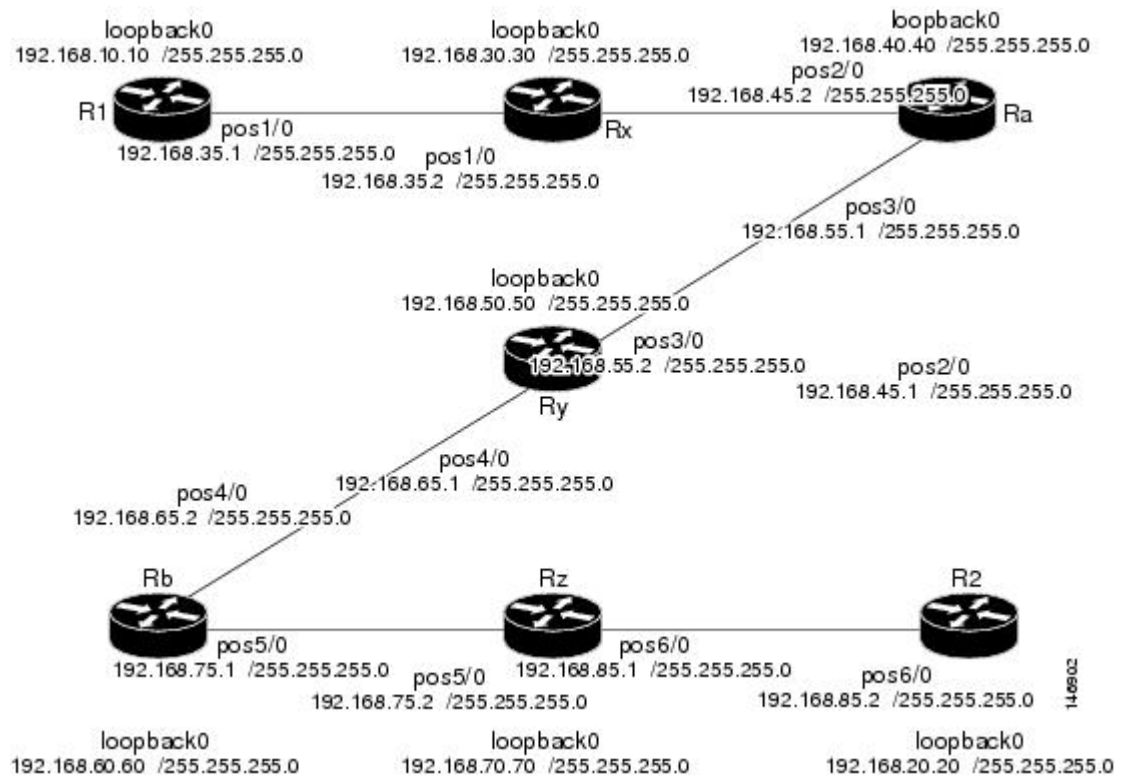
	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>tunnel-interface</i> Example: Router(config)# interface Tunnell	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<p>ip unnumbered <i>type number</i></p> <p>Example:</p> <pre>Router(config-if)# ip unnumbered Loopback 0</pre>	<p>Gives the tunnel interface an IP address.</p> <p>An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.</p>
Step 5	<p>tunnel destination <i>ip-address</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel destination 192.168.20.20</pre>	<p>Specifies the destination for a tunnel.</p> <p>You must enter the MPLS traffic engineering router ID of the destination device.</p>
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	<p>Sets the tunnel encapsulation mode to MPLS traffic engineering.</p>
Step 7	<p>tunnel mpls traffic-eng bandwidth <i>bandwidth</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 300</pre>	<p>Configures the bandwidth required for the MPLS traffic engineering tunnel.</p>
Step 8	<p>tunnel mpls traffic-eng path-option <i>number explicit</i> {name <i>path-name</i> identifier <i>path-number</i>} [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name path-Tunnell</pre>	<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 name keyword must specify the ABRs the tunnel LSP must traverse as loose hops via the next-address loose command.</p>
Step 9	<p>tunnel mpls traffic-eng autoroute destination</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng autoroute destination</pre>	<p>Automatically routes traffic through a TE tunnel.</p>
Step 10	<p>end</p> <p>Example:</p> <pre>Router(config-if)# end</pre>	<p>Returns to privileged EXEC mode.</p>

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 the figure below. It includes configuration fragments that illustrate the configurations shown in the following sections:

Figure 6: 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

Related Documents

Related Topic	Document Title
IS-IS	<ul style="list-style-type: none"> • Integrated IS-IS Routing Protocol Overview • <i>Cisco IOS IP Routing Protocols Command Reference</i>
Link protection	MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
MPLS traffic engineering commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>
OSPF	<ul style="list-style-type: none"> • <i>Cisco IOS IP Routing Protocols Command Reference</i> • Configuring OSPF

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

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>	http://www.cisco.com/techsupport

Feature Information for MPLS Traffic Engineering Interarea Tunnels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 9: Feature Information for MPLS Traffic Engineering Interarea Tunnels

Feature Name	Releases	Feature Information
MPLS Traffic Engineering: Interarea Tunnels	12.0(19)ST1 12.0(21)ST 12.2(18)S 12.2(18)SXD 12.2(27)SBC 12.2(28)SB 12.2(33)SRB 12.4(20)T 12.2(33)SRE 15.2(1)S Cisco IOS-XE Release 3.5	<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 12.2(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 MPLS-TE Autoroute Destinations feature was added.</p> <p>In 15.2(1)S the MPLS-TE Autoroute Destinations feature was added.</p> <p>In Cisco IOS-XE Release 3.5, the MPLS-TE Autoroute Destinations feature was added.</p> <p>The following commands were introduced or modified: show ip static route, show mpls traffic-eng autoroute, show mpls traffic-eng tunnels, tunnel mpls traffic-eng autoroute destination.</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.



MPLS Traffic Engineering Class-based Tunnel Selection

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, page 192](#)
- [Prerequisites for MPLS Traffic Engineering Class-based Tunnel Selection, page 192](#)
- [Restrictions for MPLS Traffic Engineering Class-based Tunnel Selection, page 192](#)
- [Information About MPLS Traffic Engineering Class-based Tunnel Selection, page 192](#)
- [How to Configure MPLS Traffic Engineering Class-based Tunnel Selection, page 200](#)
- [Configuration Examples for MPLS Traffic Engineering Class-based Tunnel Selection, page 210](#)
- [Additional References, page 217](#)
- [Feature Information for MPLS Traffic Engineering Class-based Tunnel Selection, page 217](#)
- [Glossary, page 218](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

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

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) device—Unlabeled packets that enter a Virtual Private Network (VPN) routing and forwarding (VRF) instance interface

- At a provider core (P) device—Unlabeled and MPLS-labeled packets that enter a non-VRF interface
- At a PE device 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 device imposes on the packet. Before imposing this value, the device 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

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

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:
- 3 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.
- 4 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

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.

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.

**Note**

You cannot configure FRR on a master tunnel.

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 device that is running CBTS and on transit label switch routers (LSRs).

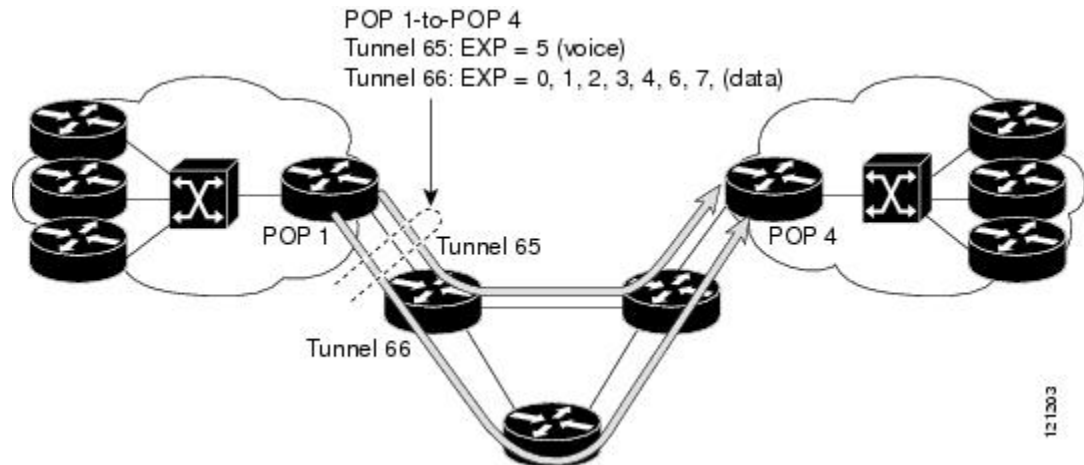
How to Configure MPLS Traffic Engineering Class-based Tunnel Selection

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

The figure below 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 7: Tunnels Transporting Different Classes of Service Between the Same Headend and Tailend



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 device to create additional tunnels from this headend to the same tailend.
10. end

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable	Enables privileged EXEC mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Device> enable</pre>	<ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example:</p> <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3	<p>interface tunnel <i>number</i></p> <p>Example:</p> <pre>Device(config)# interface tunnel 65</pre>	Configures an interface type and enters interface configuration mode.
Step 4	<p>ip unnumbered <i>type number</i></p> <p>Example:</p> <pre>Device(config-if)# ip unnumbered loopback 0</pre>	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 5	<p>tunnel destination {<i>hostname</i> <i>ip-address</i>}</p> <p>Example:</p> <pre>Device(config-if)# tunnel destination 10.10.10.12</pre>	Specifies the destination of the tunnel for this path option.
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Device(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the mode of a tunnel to MPLS for TE.
Step 7	<p>tunnel mpls traffic-eng bandwidth [sub-pool global] <i>bandwidth</i></p> <p>Example:</p> <pre>Device(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 3000</pre>	<p>Configures the bandwidth for the MPLS TE tunnel. If automatic bandwidth is configured for the tunnel, use the tunnel mpls traffic-eng bandwidth command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism.</p> <p>Note You can configure any existing MPLS TE command on these TE or DS-TE tunnels.</p>
Step 8	<p>exit</p> <p>Example:</p> <pre>Device(config-if)# exit</pre>	Returns to global configuration mode.

	Command or Action	Purpose
Step 9	Repeat steps 3 through 8 on the same headend device to create additional tunnels from this headend to the same tailend.	--
Step 10	end Example: Device(config)# end	Returns to privileged EXEC mode.

Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel

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 eng** [*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](#), on page 201.
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: Device(config)# interface tunnel 65	Configures an interface type and enters interface configuration mode.
Step 4	tunnel mpls traffic-eng eng [<i>list-of-exp-values</i>] [default] Example: Device(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	exit Example: Device(config-if)# exit	Returns to global configuration mode.
Step 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 , on page 201.	--
Step 7	end Example: Device(config-if)# end	Returns to privileged EXEC mode.

Making the MPLS TE or DS-TE Tunnels Visible for Routing



Note Alternatively, you can use static routing 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	enable Example: <pre>Router> enable</pre>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3	interface type number Example: <pre>Router(config)# interface tunnel 65</pre>	Configures an interface type and enters interface configuration mode.
Step 4	tunnel mpls traffic-eng autoroute announce Example: <pre>Router(config-if)# tunnel mpls traffic-eng autoroute announce</pre>	Specifies that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced SPF calculation.
Step 5	tunnel mpls traffic-eng autoroute metric {absolute relative} value Example: <pre>Router(config-if)# tunnel mpls traffic-eng autoroute metric relative 2</pre> Example:	Specifies the MPLS TE tunnel metric that the IGP enhanced SPF calculation uses. <p>Note Even though the value for a relative metric can be from -10 to +10, configuring a tunnel metric with a negative value is considered a misconfiguration. If 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.</p>
Step 6	end Example: <pre>Router(config-if)# end</pre>	Returns to privileged EXEC mode.

Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP

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] [protection]`
3. `show ip cef 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:

Example:

```
Device# 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
  globalpool subpool
             total allocated reservable  reservable
             -----
bw[0]:  0  1000 500
bw[1]: 10  990 490
bw[2]: 600  390 390
bw[3]:  0  390 390
bw[4]:  0  390 390
bw[5]:  0  390 390
```

Step 2 `show mpls traffic-eng tunnels number [brief] [protection]`

Use this command to display information for a specified tunneling interface:

Example:

```
Device# show mpls traffic-eng tunnels 500 brief protection

Device# 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:

Example:

```

Device# 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):

Example:

```

Device# show mpls forwarding-table
Local Outgoing Prefix Bytes tag Outgoing Next Hop
Label Label or VC or Tunnel Id switched interface
26 No Label 10.253.0.0/16 0 Et4/0/0 10.27.32.4
28 1/33 10.15.0.0/16 0 AT0/0.1 point2point
29 Pop Label 10.91.0.0/16 0 Hs5/0 point2point
 1/36 10.91.0.0/16 0 AT0/0.1 point2point
30 32 10.250.0.97/32 0 Et4/0/2 10.92.0.7
 32 10.250.0.97/32 0 Hs5/0 point2point
34 26 10.77.0.0/24 0 Et4/0/2 10.92.0.7
 26 10.77.0.0/24 0 Hs5/0 point2point
35 No Label[T] 10.100.100.101/32 0 Tu301 point2point
36 Pop Label 10.1.0.0/16 0 Hs5/0 point2point
 1/37 10.1.0.0/16 0 AT0/0.1 point2point
[T] Forwarding through a TSP tunnel.
View additional 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:

Example:

```

Device# 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)
```

Configuring a Master Tunnel

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 autoroute announce**
8. **tunnel mpls traffic-eng exp-bundle master**
9. **tunnel mpls traffic-eng exp-bundle member *tunnel-number***
10. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Device(config)# interface tunnel 65	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	ip unnumbered <i>type number</i> Example: Device(config-if)# ip unnumbered loopback 0	Enables IP processing on an interface without assigning an explicit IP address to the interface.
Step 5	tunnel destination { <i>hostname</i> <i>ip-address</i> } Example: Device(config-if)# tunnel destination 10.10.10.12	Specifies the destination of the tunnel for this path option.
Step 6	tunnel mode mpls traffic-eng Example: Device(config-if)# tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for TE.
Step 7	tunnel mpls traffic-eng autoroute announce Example: Device(config-if)# tunnel mpls traffic-eng autoroute announce	Specifies that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up
Step 8	tunnel mpls traffic-eng exp-bundle master Example: Device(config-if)# tunnel mpls traffic-eng exp-bundle master	Configures a master tunnel.
Step 9	tunnel mpls traffic-eng exp-bundle member <i>tunnel-number</i> Example: Device(config-if)# tunnel mpls traffic-eng exp-bundle member tunnell	Identifies which tunnel is a member of a master tunnel.
Step 10	exit Example: Device(config-if)# exit	Exits to global configuration mode.

Configuration Examples for MPLS Traffic Engineering Class-based Tunnel Selection

Example: Creating Multiple MPLS TE or DS-TE Tunnels from the Same Headend to the Same Tailend

The following example shows how to create multiple MPLS TE or DS-TE tunnels from the same headend to the same tailend:

```
Device(config)# interface Tunnel 65

Device(config-if)# ip numbered loopback 0
Device(config-if)# tunnel destination 10.1.1.1

Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000

Device(config-if)# ^Z
Device(config)# interface Tunnel 66

Device(config-if)# ip numbered loopback 0
Device(config-if)# tunnel destination 10.1.1.1

Device(config-if)# tunnel mode mpls traffic-eng
Device(config-if)# tunnel mpls traffic-eng bandwidth 50000
Device(config-if)# end
Device#
```

Example: Configuring EXP Values to Be Carried by Each MPLS TE or DS-TE Tunnel

The following example shows how to configure EXP values to be carried by each MPLS TE or DS-TE tunnel that you created:

```
Device(config)# interface Tunnel 65

Device(config-if)# tunnel mpls traffic-eng exp 5
Device(config-if)# ^Z
Device(config)#
Device(config)# interface Tunnel 66

Device(config-if)# tunnel mpls traffic-eng exp 0 1 2 3 4 6 7
Device(config-if)# end
Device#
```

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.

Example: Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP

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:

```

Device# 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)
      Global Pool          Sub Pool
      Total Allocated    Reservable    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]:               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)
      Global Pool          Sub Pool
      Total Allocated    Reservable    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
Device#
Device# 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

```

Example: Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP

```

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 BW (kbps)	Global Pool Reservable BW (kbps)	Sub Pool Reservable 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 BW (kbps)	Global Pool Reservable BW (kbps)	Sub Pool Reservable 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

```

Device#

```

The **show mpls traffic-eng tunnels** command output displays information about a tunnel:

```

Device# 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
Device# 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
Device# 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
Device# show mpls traffic-eng tunnels tunnel4
Name: Router_t4                               (Tunnel4) Destination: 10.0.0.9

```

Example: Verifying That the MPLS TE or DS-TE Tunnels Are Operating and Announced to the IGP

```

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:

```

Device# show ip cef tunnell 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, Tunnell, 0 dependencies
  traffic share 1
  next hop 0.0.0.0, Tunnell
  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
Device# 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
Device# 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
Device# 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

```

Example: Configuring a Master Tunnel

```
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:

```
Device# show mpls forwarding-table detail
Local  Outgoing  Prefix      Bytes tag  Outgoing   Next Hop
tag    tag or VC  or Tunnel Id  switched  interface
Device#
Device# show mpls forwarding-table 10.0.0.9 detail
Local  Outgoing  Prefix      Bytes tag  Outgoing   Next Hop
tag    tag or VC  or Tunnel Id  switched  interface
Tun hd  Untagged  10.0.0.9/32    0          Tu1         point2point
MAC/Encaps=14/18, MRU=1500, Tag Stack{12304}, via Fa6/0
00027D884001000ED70178A98847 03010000
No output feature configured
  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
00027D884001000ED70178A98847 03011000
No output feature configured
  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
00027D884001000ED70178A98847 03012000
No output feature configured
  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
00027D884001000ED70178A98847 03013000
No output feature configured
  Per-exp selection: 0 6 7
Device#
```

The **show mpls traffic-eng autoroute** command output displays tunnels that are announced to the IGP:

```
Device# 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)
Device#
```

Example: Configuring a Master Tunnel

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 mode mpls traffic-eng autoroute announce
tunnel mpls traffic-eng exp-bundle master
tunnel mpls traffic-eng exp-bundle member Tunnel20000
tunnel mpls traffic-eng exp-bundle member Tunnel20001
tunnel mpls traffic-eng exp-bundle member Tunnel20002
tunnel mpls traffic-eng exp-bundle member Tunnel20003
tunnel mpls traffic-eng exp-bundle member Tunnel20004
tunnel mpls traffic-eng exp-bundle member Tunnel20005
```

Additional References

Related Documents

Related Topic	Document Title
MPLS traffic engineering commands	<i>Multiprotocol Label Switching Command Reference</i>

Technical Assistance

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

Feature Information for MPLS Traffic Engineering Class-based Tunnel Selection

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 10: 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 12.2(33)SRA 12.2(32)SY 12.2(33)SXH 12.4(20)T Cisco IOS XE Release 3.6S	<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"> • tunnel mpls traffic-eng exp-bundle master • tunnel mpls traffic-eng exp-bundle member • show mpls traffic-eng exp <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> <p>In Cisco IOS XE Release 3.6S, 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 device 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 device 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. 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.



MPLS Traffic Engineering Automatic Bandwidth Adjustment for TE Tunnels

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, page 221](#)
- [Prerequisites for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels, page 222](#)
- [Restrictions for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels, page 222](#)
- [Information About MPLS TE Automatic Bandwidth Adjustment for TE Tunnels, page 222](#)
- [How to Configure MPLS TE Automatic Bandwidth Adjustment for TE Tunnels, page 223](#)
- [Configuration Examples for MPLS TE Automatic Bandwidth Adjustments for TE Tunnels, page 237](#)
- [Additional References, page 238](#)
- [Feature Information for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels, page 240](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

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.
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

Information About MPLS TE Automatic Bandwidth Adjustment for TE Tunnels

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

Configuring a Device to Support Traffic Engineering Tunnels

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip cef distributed`
4. `mpls traffic-eng tunnels`
5. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: <code>Router> enable</code>	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>ip cef distributed</code> Example: <code>Router(config)# ip cef distributed</code>	Enables distributed Cisco Express Forwarding operation.
Step 4	<code>mpls traffic-eng tunnels</code> Example: <code>Router(config)# mpls traffic-eng tunnels</code>	Enables the MPLS traffic engineering tunnel feature on a device.

	Command or Action	Purpose
Step 5	exit Example: 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

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

	Command or Action	Purpose
Step 3	router isis Example: Router(config)# router isis	Enables IS-IS routing and specifies an IS-IS process for IP, and enters router configuration mode.
Step 4	mpls traffic-eng level-1 Example: Router(config-router)# mpls traffic-eng level-1	Turns on MPLS TE for IS-IS level 1.
Step 5	mpls traffic-eng router-id loopback0 Example: 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	metric-style wide Example: Router(config-router)# metric-style wide	Configures a router to generate and accept only new-style type, length, value objects (TLVs).
Step 7	exit Example: Router(config-router)# exit	Exits to global configuration mode.
Step 8	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

Configuring OSPF for MPLS Traffic Engineering

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	router ospf process-id Example: Router(config)# router ospf 200	Configures an OSPF routing process for IP and enters router configuration mode. <ul style="list-style-type: none"> • 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.
Step 4	mpls traffic-eng area number Example: Router(config-router)# mpls traffic-eng area 0	Turns on MPLS TE for the indicated OSPF area.
Step 5	mpls traffic-eng router-id loopback0 Example: 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.

	Command or Action	Purpose
Step 6	exit Example: Router(config-router)# exit	Exits to global configuration mode.
Step 7	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

Configuring Bandwidth on Each Link That a Tunnel Crosses

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

	Command or Action	Purpose
Step 3	interface <i>type number</i> Example: <pre>Router(config)# interface FastEthernet 0/0/0</pre>	Configures an interface type and enters interface configuration mode.
Step 4	mpls traffic-eng tunnels Example: <pre>Router(config-if)# mpls traffic-eng tunnels</pre>	Enables MPLS TE tunnels on an interface.
Step 5	ip rsvp bandwidth [<i>interface-kbps</i>] [<i>single-flow-kbps</i>] [sub-pool kbps] Example: <pre>Router(config-if)# ip rsvp bandwidth 1000 100</pre>	Enables Resource Reservation Protocol (RSVP) for IP on an interface. <ul style="list-style-type: none"> • 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. • 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.
Step 6	exit Example: <pre>Router(config-if)# exit</pre>	Exits to global configuration mode.
Step 7	exit Example: <pre>Router(config)# exit</pre>	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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	ip unnumbered <i>interface-type interface-number</i> Example: Router(config-if)# ip unnumbered loopback 0	Gives the tunnel interface an IP address that is the same as that of interface Loopback0. <ul style="list-style-type: none"> • An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link. Note This command is not effective until Loopback0 has been configured with an IP address.
Step 5	tunnel destination <i>ip-address</i>	Specifies the destination for a tunnel.

	Command or Action	Purpose
	<p>Example:</p> <pre>Router(config-if)# tunnel destination 10.3.3.3</pre>	<ul style="list-style-type: none"> The destination must be the MPLS TE router ID of the destination device.
Step 6	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the encapsulation mode of the tunnel to MPLS TE.
Step 7	<p>tunnel mpls traffic-eng bandwidth <i>bandwidth</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 250</pre>	<p>Configures the bandwidth for the MPLS TE tunnel.</p> <ul style="list-style-type: none"> 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. If automatic bandwidth is configured for the tunnel, the tunnel mpls traffic-eng bandwidth command configures the initial tunnel bandwidth, which will be adjusted by the autobandwidth mechanism. <p>Note If you configure a tunnel's bandwidth with the tunnel mpls traffic-eng bandwidth command and the minimum amount of automatic bandwidth with the tunnel mpls traffic-eng auto-bw command, the minimum amount of automatic bandwidth adjustment is the lower of those two configured values.</p>
Step 8	<p>tunnel mpls traffic-eng path-option [protect] <i>preference-number</i>{dynamic explicit {name <i>path-name</i> <i>path-number</i>}} [lockdown]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link</pre>	<p>Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the TE topology database.</p> <ul style="list-style-type: none"> A dynamic path is used if an explicit path is currently unavailable.
Step 9	<p>exit</p> <p>Example:</p> <pre>Router(config-if)# exit</pre>	Exits to global configuration mode.
Step 10	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	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	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>mpls traffic-eng auto-bw timers [<i>frequency seconds</i>]</p> <p>Example:</p> <pre>Router(config)# mpls traffic-eng auto-bw timers frequency 300</pre>	<p>Enables automatic bandwidth adjustment on a platform and begins sampling the output rate for tunnels that have been configured for automatic bandwidth adjustment.</p> <ul style="list-style-type: none"> The frequency 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.
Step 4	<p>no mpls traffic-eng auto-bw timers</p> <p>Example:</p> <pre>Router(config)# no mpls traffic-eng auto-bw timers</pre>	<p>(Optional) Disables automatic bandwidth adjustment on a platform.</p> <ul style="list-style-type: none"> Use the no version of the command, which terminates output rate sampling and bandwidth adjustment for tunnels. In addition, the no form of the command restores the configured bandwidth for each tunnel where the configured bandwidth is determined as follows: <ul style="list-style-type: none"> If the tunnel bandwidth was explicitly configured via the tunnel mpls traffic-eng bandwidth command after the running configuration was written to the startup configuration, the configured bandwidth is the bandwidth specified by that command. Otherwise, the configured bandwidth is the bandwidth specified for the tunnel in the startup configuration.
Step 5	<p>exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits to privileged EXEC mode.</p>

Enabling Automatic Bandwidth Adjustment for a Tunnel

SUMMARY STEPS

- enable
- configure terminal
- interface tunnel *number*
- 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*]
- exit
- exit

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	tunnel mpls traffic-eng auto-bw [collect-bw] [frequency <i>seconds</i>] [adjustment-threshold <i>percent</i>] [overflow-limit <i>number</i>] [overflow-threshold <i>percent</i>] [max-bw <i>kbps</i>] [min-bw <i>kbps</i>] Example: 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	exit Example: Router(config-if)# exit	Exits to global configuration mode.
Step 6	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

Configuring the Interval for Computing the Tunnel Average Output Rate

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	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	load-interval <i>seconds</i> Example: Router(config-if)# load-interval 90	Configures the interval over which the input and output rates for the interface are averaged. <ul style="list-style-type: none"> • 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.
Step 5	exit Example: Router(config-if)# exit	Exits to global configuration mode.

	Command or Action	Purpose
Step 6	exit Example: Router(config)# exit	Exits to privileged EXEC mode.

Verifying Automatic Bandwidth Configuration

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:

Example:

```
Router# show mpls traffic-eng tunnels
Name:tagsw4500-9_t1 (Tunnell) 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.

Example:

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:

Example:

```

Router# show running-config
.
.
.
interface tunnell
 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

```

Example:

·
·
·

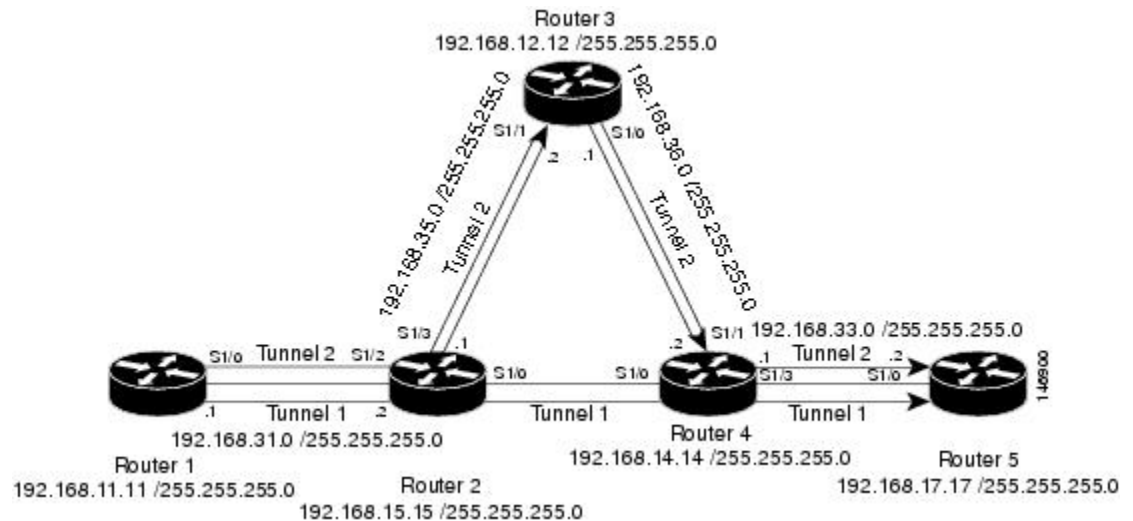
The sample output from the **show running-config** command shows that the value 1500, in the **tunnel mpls traffic-eng bandwidth 1500** command, changes after an adjustment is made.

Example:

Configuration Examples for MPLS TE Automatic Bandwidth Adjustments for TE Tunnels

The figure below 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 8: Sample MPLS Traffic Engineering Tunnel Configuration



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.

Example: Configuring MPLS Traffic Engineering Automatic Bandwidth

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
```

Example: Tunnel Configuration for Automatic Bandwidth

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 tunnell
 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

Related Documents

Related Topic	Document Title
IS-IS and OSPF commands	<i>Cisco IOS IP Routing Protocols Command Reference</i>
MPLS commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>
Quality of service solutions commands	<i>Cisco IOS Quality of Service Solutions Command Reference</i>
Quality of service solutions configuration	Quality of Service Overview

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

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>	http://www.cisco.com/techsupport

Feature Information for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 11: Feature Information for MPLS TE Automatic Bandwidth Adjustment for TE Tunnels

Feature Name	Releases	Feature Information
MPLS Traffic Engineering Automatic Bandwidth Adjustment for TE Tunnels	12.2(33)SRE	<p>The MPLS Traffic Engineering Automatic Bandwidth Adjustment for TE Tunnels feature provides the means to automatically adjust the bandwidth allocation for traffic engineering tunnels based on their measured traffic load. The configured bandwidth in the running configuration is changed due to the automatic bandwidth behavior.</p> <p>In Cisco IOS Release 12.2(33)SRE, this feature was introduced.</p> <p>The following commands were introduced or modified to support automatic bandwidth adjustment threshold and overflow threshold: mpls traffic-eng lsp attributes, show mpls traffic-eng tunnels, tunnel mpls traffic-eng auto-bw.</p>



MPLS Traffic Engineering Tunnel Source

The Multiprotocol Label Switching (MPLS) Traffic Engineering (TE): Tunnel Source feature allows you to specify the IP address assigned to an interface as the source IP address for control packets. The default behavior is to use the router ID configured in the Interior Gateway Protocol (IGP) using the **mpls traffic-eng router-id** command.

- [Finding Feature Information, page 241](#)
- [Prerequisites for MPLS Traffic Engineering Tunnel Source, page 241](#)
- [Restrictions for MPLS Traffic Engineering Tunnel Source, page 242](#)
- [Information About MPLS Traffic Engineering Tunnel Source, page 242](#)
- [How to Configure MPLS Traffic Engineering Tunnel Source, page 242](#)
- [Configuration Examples for MPLS Traffic Engineering Tunnel Source, page 245](#)
- [Additional References, page 246](#)
- [Feature Information for MPLS Traffic Engineering Tunnel Source, page 247](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and 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 table at the end of this module.

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

Prerequisites for MPLS Traffic Engineering Tunnel Source

- You can configure tunnel source only for MPLS-TE tunnels.
- Understand how to configure TE tunnels. See the [Additional References, on page 246](#).

Restrictions for MPLS Traffic Engineering Tunnel Source

- The configuration of other types of tunnels are not affected by this feature.
- Configuring a tunnel source affects the control traffic and not the traffic forwarded in the dataplane on this tunnel.

Information About MPLS Traffic Engineering Tunnel Source

When you configure an MPLS TE tunnel, the address specified in the **tunnel source** command is used as the source IP address for control traffic to signal the tunnel. The source IP address overrides the default IP address taken from the IGP command **mpls traffic-eng router-id**.

MPLS Traffic Engineering Tunnel Source Usage Guidelines

- Specifying a new source for an established tunnel causes the tunnel to be withdrawn and re-established.
- The tunnel source may be configured as an IP address or as an interface. If an interface is specified, it must have an associated IP address.

How to Configure MPLS Traffic Engineering Tunnel Source

Configuring MPLS Traffic Engineering Tunnel Source

You can configure the tunnel source as an IP address or as an interface. If you configure the tunnel source as an interface, then you should configure an IP address for the interface.

To specify a tunnel source for an MPLS TE tunnel, perform the following steps:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel *number***
4. **ip unnumbered *interface-name interface-number***
5. **no ip directed-broadcast**
6. **tunnel source {*ip-address* | *interface-type interface-number*}**
7. **tunnel destination {*host-name* | *ip-address* | *ipv6-address*}**
8. **tunnel mode mpls traffic-eng**
9. **tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]**
10. **tunnel mpls traffic-eng bandwidth *bandwidth***
11. **tunnel mpls traffic-eng affinity *affinity value* mask *mask-value***
12. **tunnel mpls traffic-eng path-option *number* explicit name *explicit-path-name***
13. **tunnel mpls traffic-eng autoroute announce**
14. **end**
15. show ip rsvp sender

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface tunnel <i>number</i> Example: Router(config)# interface tunnel 1	Configures a tunnel interface and enters interface configuration mode.
Step 4	ip unnumbered <i>interface-name interface-number</i> Example: Router(config-if)# ip unnumbered loopback0	Configures an unnumbered IP interface, which enables IP processing without an explicit address. <ul style="list-style-type: none"> • An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link.

	Command or Action	Purpose
Step 5	<p>no ip directed-broadcast</p> <p>Example:</p> <pre>Router(config-if)# no ip directed-broadcast</pre>	Disables the translation of a directed broadcast to physical broadcasts.
Step 6	<p>tunnel source {<i>ip-address</i> <i>interface-type</i> <i>interface-number</i>}</p> <p>Example:</p> <pre>Router(config-if)# tunnel source loopback1</pre>	Configures the tunnel source.
Step 7	<p>tunnel destination {<i>host-name</i> <i>ip-address</i> <i>ipv6-address</i>}</p> <p>Example:</p> <pre>Router(config-if)# tunnel destination 192.168.2.1</pre>	<p>Specifies the destination for a tunnel.</p> <ul style="list-style-type: none"> The destination must be the MPLS TE router ID of the destination device.
Step 8	<p>tunnel mode mpls traffic-eng</p> <p>Example:</p> <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>	Sets the encapsulation mode of the tunnel to MPLS TE.
Step 9	<p>tunnel mpls traffic-eng priority <i>setup-priority</i> [<i>hold-priority</i>]</p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng priority 1 1</pre>	<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"> The setup-priority argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted. 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. The hold-priority 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. Valid values are from 0 to 7, where a lower number indicates a higher priority.
Step 10	<p>tunnel mpls traffic-eng bandwidth <i>bandwidth</i></p> <p>Example:</p> <pre>Router(config-if)# tunnel mpls traffic-eng bandwidth 5000</pre>	Configures the bandwidth for the MPLS traffic engineering tunnel.

	Command or Action	Purpose
Step 11	tunnel mpls traffic-eng affinity <i>affinity value</i> mask <i>mask-value</i> Example: Router(config-if)# tunnel mpls traffic-eng affinity 0x0 mask 0x0	Configures the properties an MPLS TE tunnel requires in its links.
Step 12	tunnel mpls traffic-eng path-option <i>number</i> explicit name <i>explicit-path-name</i> Example: Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name BEST-WAY	Configures a path option for an MPLS TE tunnel. <ul style="list-style-type: none"> • The explicit keyword specifies that the path of the LSP is an IP explicit path.
Step 13	tunnel mpls traffic-eng autoroute announce Example: Router(config-if)# tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel in its enhanced shortest path first (SPF) calculation.
Step 14	end Example: Router(config-if)# end	Exits interface configuration modes and enters privileged EXEC mode.
Step 15	show ip rsvp sender Example: Router# show ip rsvp sender	Displays the IP address used as the source for tunnel control traffic.

Configuration Examples for MPLS Traffic Engineering Tunnel Source

MPLS Traffic Engineering Tunnel Source Example

The output of the **show running-config** command displays the tunnel source configuration. If the **tunnel source** command is not configured, the IP address specified in the IGP command **mpls traffic-eng router-id** is used.

```
Router# show running-config
```

```

Building configuration...
Current configuration: 3969 bytes
!
!
interface Tunnell
 ip unnumbered loopback0
 tunnel source loopback1
 tunnel mode mpls traffic-eng
 tunnel destination 192.168.2.1
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 5000
 tunnel mpls traffic-eng affinity 0x0 mask 0x0
 tunnel mpls traffic-eng path-option 1 explicit name BEST-WAY
 tunnel mpls traffic-eng autoroute announce
!
...
router isis
 net 49.0000.0001.0000.0001.00
 is-type level-1
 metric-style wide
 mpls traffic-eng router-id Ethernet4/0/1
 mpls traffic-eng level-1
!

```

The following sample output from the **show ip rsvp sender** command displays that the source IP address of the loopback interface used for tunnel control traffic:

```

Router# show ip rsvp sender
To          From          Pro DPort Sport   Prev Hop      I/F      BPS
192.168.2.1 192.168.42.2  0   1    13    192.168.42.10 Et0/0 SE LOAD 5M

```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MPLS commands	<i>Cisco IOS Multiprotocol Label Switching Command Reference</i>
MPLS TE automatic bandwidth adjustment for TE tunnels configuration tasks	MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels module
MPLS TE - LSP Attributes	MPLS Traffic Engineering--LSP Attributes module
MPLS TE: Path Protection	MPLS Traffic Engineering (TE) - Path Protection module

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • None 	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

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

Feature Information for MPLS Traffic Engineering Tunnel Source

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 12: Feature Information for MPLS Traffic Engineering: Tunnel Source

Feature Name	Releases	Feature Information
MPLS Traffic Engineering: Tunnel Source	12.2(33)SRD 12.2(33)SXI2 12.2(52)SE 15.0(1)M	<p>The MPLS Traffic Engineering: Tunnel source feature allows you to specify the IP address assigned to an interface as the source IP address for control packets. The default behavior is to use the router ID configured in the IGP using the mpls traffic-eng router-id command.</p> <p>The following command was introduced or modified: tunnel source.</p>