CONTENTS

CHAPTER 1

MPLS Traffic Engineering--Fast Reroute Link and Node Protection  1

Finding Feature Information  1

Prerequisites for MPLS Traffic Engineering--Fast Reroute Link and Node Protection  2

Restrictions for MPLS Traffic Engineering--Fast Reroute Link and Node Protection  2

Information About MPLS Traffic Engineering--Fast Reroute Link and Node Protection  3

Fast Reroute  3

Link Protection  3

Node Protection  3

Bandwidth Protection  4

RSVP Hello  5

RSVP Hello Operation  5

Hello Instance  5

Features of MPLS Traffic Engineering--Fast Reroute Link and Node Protection  6

Backup Tunnel Support  6

Backup Bandwidth Protection  7

RSVP Hello  7

Fast Reroute Operation  8

Fast Reroute Activation  8

Backup Tunnels Terminating at Different Destinations  8

Backup Tunnels Terminating at the Same Destination  9

Backup Tunnel Selection Procedure  9

Bandwidth Protection  10

Load Balancing on Limited-Bandwidth Backup Tunnels  10

Load Balancing on Unlimited-Bandwidth Backup Tunnels  11

Pool Type and Backup Tunnels  12

Tunnel Selection Priorities  12

Bandwidth Protection Considerations  14

How to Configure MPLS Traffic Engineering—Fast Reroute Link and Node Protection  17
Contents

Enabling Fast Reroute on LSPs 17
Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop 18
Assigning Backup Tunnels to a Protected Interface 20
Associating Backup Bandwidth and Pool Type with a Backup Tunnel 21
Configuring Backup Bandwidth Protection 23
Configuring an Interface for Fast Link and Node Failure Detection 24
Verifying That Fast Reroute Is Operational 25
Troubleshooting Tips 30
Configuration Examples for MPLS Traffic Engineering—Fast Reroute Link and Node Protection 33
Enabling Fast Reroute for all Tunnels Example 33
Creating an NHOP Backup Tunnel Example 33
Creating an NNHOP Backup Tunnel Example 34
Assigning Backup Tunnels to a Protected Interface Example 34
Associating Backup Bandwidth and Pool Type with Backup Tunnels Example 34
Configuring Backup Bandwidth Protection Example 35
Configuring an Interface for Fast Link and Node Failure Detection Example 35
Configuring RSVP Hello and POS Signals Example 35
Additional References 36
Command Reference 37
Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection 38
Glossary 40

CHAPTER 2

MPLS TE Link and Node Protection with RSVP Hellos Support 43
Finding Feature Information 44
Prerequisites for MPLS TE Link and Node Protection with RSVP Hellos Support 44
Restrictions for MPLS TE Link and Node Protection with RSVP Hellos Support 44
Information About MPLS TE Link and Node Protection with RSVP Hellos Support 45
Fast Reroute 45
Link Protection 45
Node Protection 45
Bandwidth Protection 46
Fast Tunnel Interface Down Detection 47
RSVP Hello 47
RSVP Hello Operation 47
Hello Instance 47
Hello Commands 48

Features of MPLS TE Link and Node Protection with RSVP Hellos Support 48
Backup Tunnel Support 48
Backup Bandwidth Protection 49
RSVP Hello 50

Fast Reroute Operation 50
Fast Reroute Activation 50
Backup Tunnels Terminating at Different Destinations 51
Backup Tunnels Terminating at the Same Destination 52
Backup Tunnel Selection Procedure 52
Bandwidth Protection 53
Load Balancing on Limited-bandwidth Backup Tunnels 53
Load Balancing on Unlimited-bandwidth Backup Tunnels 54
Pool Type and Backup Tunnels 54
Tunnel Selection Priorities 54
Bandwidth Protection Considerations 57
Using Backup Tunnels with Explicitly Signaled Bandwidth 57
Using Backup Tunnels Signaled with Zero Bandwidth 59

How to Configure MPLS TE Link and Node Protection with RSVP Hellos Support 60
Enabling Fast Reroute on LSPs 60
Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop 61
Assigning Backup Tunnels to a Protected Interface 63
Associating Backup Bandwidth and Pool Type with a Backup Tunnel 65
Configuring Backup Bandwidth Protection 66
Configuring an Interface for Fast Link and Node Failure Detection 66
Configuring an Interface for Fast Tunnel Interface Down 67
Verifying That Fast Reroute Is Operational 68
Troubleshooting Tips 74

Config Examples for MPLS TE Link and Node Protection with RSVP Hellos Support 77
Enabling Fast Reroute for All Tunnels Example 77
Creating an NHOP Backup Tunnel Example 78
Creating an NNHOP Backup Tunnel Example 78
Assigning Backup Tunnels to a Protected Interface Example 78
CHAPTER 3

MPLS Traffic Engineering (TE) Path Protection 87

Finding Feature Information 87
Prerequisites for MPLS Traffic Engineering (TE) Path Protection 87
Restrictions for MPLS Traffic Engineering (TE) Path Protection 88
Information About MPLS Traffic Engineering (TE) Path Protection 88
  Traffic Engineering Tunnels 88
  Path Protection 88
  Enhanced Path Protection 89
  ISSU 89
  NSF/SSO 89
How to Configure MPLS Traffic Engineering (TE) Path Protection 90
Regular Path Protection Configuration Tasks 90
  Configuring Explicit Paths for Secondary Paths 90
  Assigning a Secondary Path Option to Protect a Primary Path Option 92
  Verifying the Configuration of MPLS Traffic Engineering Path Protection 93
Enhanced Path Protection Configuration Tasks 96
  Creating a Path Option List 97
  Assigning a Path Option List to Protect a Primary Path Option 98
  Verifying the Configuration of MPLS Traffic Engineering Path Protection 100
Configuration Examples for MPLS Traffic Engineering (TE): Regular Path Protection 103
  Example Configuring Explicit Paths for Secondary Paths 103
  Example Assigning a Secondary Path Option to Protect a Primary Path Option 104
  Example Configuring Tunnels Before and After Path Protection 104
Configuration Examples for MPLS Traffic Engineering (TE): Enhanced Path Protection 108
  Creating a Path Option List: Example 108
CHAPTER 6

MPLS Traffic Engineering Shared Risk Link Groups 151

Finding Feature Information 151

Prerequisites for MPLS Traffic Engineering Shared Risk Link Groups 152

Restrictions for MPLS Traffic Engineering Shared Risk Link Groups 152

Information About MPLS Traffic Engineering Shared Risk Link Groups 152

MPLS Traffic Engineering Brief Overview 152

MPLS Traffic Engineering Shared Risk Link Groups 152

Fast Reroute Protection for MPLS TE SRLGs 154

Autotunnel Backup for MPLS TE SRLGs 155

How to Configure MPLS Traffic Engineering Shared Risk Link Groups 157

Configuring MPLS TE SRLG Membership of Each Link That Has a Shared Risk with Another Link 157
Configuring the Routers That Automatically Create Backup Tunnels to Avoid MPLS TE SRLGs 158

Verifying the MPLS Traffic Engineering Shared Risk Link Groups Configuration 159

Configuration Examples for MPLS Traffic Engineering Shared Risk Link Groups 165

Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link Example 165

Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs Example 166

Additional References 167

Feature Information for MPLS Traffic Engineering Shared Risk Link Groups 169

Glossary 172

CHAPTER 7  MPLS Traffic Engineering Inter-AS TE 175

Finding Feature Information 176

Prerequisites for MPLS Traffic Engineering Inter-AS TE 176

Restrictions for MPLS Traffic Engineering Inter-AS TE 176

Information About MPLS Traffic Engineering Inter-AS TE 177

MPLS Traffic Engineering Tunnels 177

Multiarea Network Design 177

Fast Reroute 177

ASBR Node Protection 178

Loose Path Reoptimization 182

ASBR Forced Link Flooding 183

Link Flooding 186

How to Configure MPLS Traffic Engineering Inter-AS TE 186

Configuring Loose Hops 186

Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link 186

Configuring a Route to Reach the Remote ASBR 188

Configuring a Static Route from the MP to the PLR 188

Configuring ASBR Forced Link Flooding 189

Configuring the Inter-AS Link as a Passive Interface Between Two ASBRs 189

Creating LSPs Traversing the ASBRs 190

Configuring Multiple Neighbors on a Link 192

Troubleshooting Tips 193

Verifying the Inter-AS TE Configuration 193
CHAPTER 1

MPLS Traffic Engineering--Fast Reroute Link and Node Protection

The MPLS Traffic Engineering--Fast Reroute Link and Node Protection feature provides link protection (backup tunnels that bypass only a single link of the label-switched path (LSP)), node protection (backup tunnels that bypass next-hop nodes along LSPs), and Fast Reroute (FRR) features.

- Finding Feature Information, page 1
- Prerequisites for MPLS Traffic Engineering--Fast Reroute Link and Node Protection, page 2
- Restrictions for MPLS Traffic Engineering--Fast Reroute Link and Node Protection, page 2
- Information About MPLS Traffic Engineering--Fast Reroute Link and Node Protection, page 3
- How to Configure MPLS Traffic Engineering—Fast Reroute Link and Node Protection, page 17
- Configuration Examples for MPLS Traffic Engineering—Fast Reroute Link and Node Protection, page 33
- Additional References, page 36
- Command Reference, page 37
- Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection, page 38
- Glossary, page 40

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--Fast Reroute Link and Node Protection

Your network must support the following Cisco IOS features:

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

Your network must support at least one of the following protocols:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

Before configuring FRR link and node protection, it is assumed that you have done the following tasks but you do not have to already have configured MPLS traffic engineering (TE) tunnels:

- Enabled MPLS TE on all relevant routers and interfaces
- Configured MPLS TE tunnels

Restrictions for MPLS Traffic Engineering--Fast Reroute Link and Node Protection

- Interfaces must use MPLS Global Label Allocation.
- Backup tunnel headend and tailend routers must implement FRR as described in draft-pan-rsvp-fastreroute-00.txt.
- Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.
- LSPs that are actively using backup tunnels are not considered for promotion. If an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.
- You cannot enable FRR Hellos on a router that also has Resource Reservation Protocol (RSVP) Graceful Restart enabled.
- (Applicable only to Release 12.2.) You cannot enable primary one-hop autotunnels, backup autotunnels, or autotunnel mesh groups on a router that is also configured with stateful switchover (SSO) redundancy. This restriction does not prevent an MPLS TE tunnel that is automatically configured by TE autotunnel from being successfully recovered by any midpoint router along the LSP’s path if the router experiences an SSO switchover.
- MPLS TE LSPs that are fast reroutable cannot be successfully recovered if the LSPs are FRR active and the Point of Local Repair (PLR) router experiences an SSO.
- When SSO (stateful switchover) occurs on a router, the switchover process must complete before FRR (fast reroute) can complete successfully. In a testing environment, allow approximately 2 minutes for
TE SSO recovery to complete before manually triggering FRR. To check the TE SSO status, use the `show ip rsvp high-availability summary` command. Note the status of the HA state field.

- When SSO is in the process of completing, this field will display 'Recovering'.
- When the SSO process has completed, this field will display 'Active'.

Information About MPLS Traffic Engineering--Fast Reroute Link and Node Protection

Fast Reroute

Fast Reroute (FRR) is a mechanism for protecting MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or node.

Link Protection

Backup tunnels that bypass only a single link of the LSP’s path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP’s traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP’s next hop beyond the point of failure. The figure below illustrates an NHOP backup tunnel.

Figure 1: NHOP Backup Tunnel

![Figure 1: NHOP Backup Tunnel](image)

Node Protection

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node.
to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

The figure below illustrates an NNHOP backup tunnel.

Figure 2: NNHOP Backup Tunnel

If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes are the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.
- Primary LSP is modified so that FRR is disabled. (The `no mpls traffic-eng fast-reroute` command is entered.)

### Bandwidth Protection

NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected. For information about mapping tunnels and assigning backup bandwidth, see the Backup Tunnel Selection Procedure.

LSPs that have the "bandwidth protection desired" bit set have a higher right to select backup tunnels that provide bandwidth protection; that is, those LSPs can preempt other LSPs that do not have that bit set. For more information, see the Bandwidth Protection, on page 4.
RSVP Hello

RSVP Hello Operation
RSVP Hello enables RSVP nodes to detect when a neighboring node is not reachable. This provides node-to-node failure detection. When such a failure is detected, it is handled in a similar manner as a link-layer communication failure.

RSVP Hello can be used by FRR when notification of link-layer failures is not available (for example, with Ethernet), or when the failure detection mechanisms provided by the link layer are not sufficient for the timely detection of node failures.

A node running Hello sends a Hello Request to a neighboring node every interval. If the receiving node is running Hello, it responds with Hello Ack. If four intervals pass and the sending node has not received an Ack or it receives a bad message, the sending node declares that the neighbor is down and notifies FRR.

There are two configurable parameters:
- Hello interval--Use the `ip rsvp signalling hello refresh interval` command.
- Number of acknowledgment messages that are missed before the sending node declares that the neighbor is down--Use the `ip rsvp signalling hello refresh misses` command

Hello Instance
A Hello instance implements RSVP Hello for a given router interface IP address and remote IP address. A large number of Hello requests are sent; this puts a strain on the router resources. Therefore, create a Hello instance only when it is necessary and delete it when it is no longer needed.

There are two types of Hello instances:
- Hello Instance, on page 5
- Hello Instance, on page 5

Active Hello Instances
If a neighbor is unreachable when an LSP is ready to be fast rerouted, an active Hello instance is needed. Create an active Hello instance for each neighbor with at least one LSP in this state.

Active Hello instances periodically send Hello Request messages, and expect Hello Ack messages in response. If the expected Ack message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (lost). LSPs traversing that neighbor may be fast rerouted.

If there is a Hello instance with no LSPs for an unreachable neighbor, do not delete the Hello instance. Convert the active Hello instance to a passive Hello instance because there may be an active instance on the neighboring router that is sending Hello requests to this instance.

Passive Hello Instances
Passive Hello instances respond to Hello Request messages (sending Ack messages), but do not initiate Hello Request messages and do not cause LSPs to be fast rerouted. A router with multiple interfaces can run multiple Hello instances to different neighbors or to the same neighbor.
A passive Hello instance is created when a Hello Request is received from a neighbor with a source IP address/destination IP address pair in the IP header for which a Hello instance does not exist. Delete passive instances if no Hello messages are received for this instance within 10 minutes.

Features of MPLS Traffic Engineering--Fast Reroute Link and Node Protection

Backup Tunnel Support

Backup tunnel support has the following capabilities:

Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR
Backup tunnel that terminates at the next-next hop router to protect both the downstream link and node to protect link and node failures. For more detailed information, see the Node Protection, on page 45.

Multiple Backup Tunnels Can Protect the Same Interface
There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for Node Protection requires supporting multiple backup tunnels per protected interface. These backup tunnels can terminate at the same destination or at different destinations. That is, for a given protected interface, you can configure multiple NHOP or NNHOP backup tunnels. This allows redundancy and load balancing.

In addition to being required for Node Protection, this feature provides the following benefits:

• Redundancy--If one backup tunnel is down, other backup tunnels protect LSPs.

• Increased backup capacity--If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels). For a more detailed explanation, see the Backup Tunnel Selection Procedure.

Examples are shown in the Backup Tunnels Terminating at Different Destinations, on page 51 and the Backup Tunnels Terminating at the Same Destination.

Scalability

A backup tunnel is scalable because it can protect multiple LSPs and multiple interfaces. It provides many-to-one (N:1) protection, which has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

Example of 1:1 protection: When 5,000 backup tunnels protect 5,000 LSPs, each router along the backup path must maintain state for an additional 5,000 tunnels.

Example of N:1 protection: When one backup tunnel protects 5,000 LSPs, each router along the backup path maintains one additional tunnel.
**Backup Bandwidth Protection**

Backup bandwidth protection allows you to give LSPs carrying certain kinds of data (such as voice) priority for using backup tunnels. Backup bandwidth protection has the following capabilities:

**Bandwidth Protection on Backup Tunnels**

Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.

**Bandwidth Pool Specifications for Backup Tunnels**

You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using subpool bandwidth can use them or only LSPs that use global-pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could not provide bandwidth protection.

**Semidynamic Backup Tunnel Paths**

The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature that was added in Release 12.0(14)ST. If you use this feature, semidynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semidynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.

**Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection**

In case there are not enough NHOP or NNHOP backup tunnels or they do not have enough backup bandwidth to protect all LSPs, you can give an LSP priority in obtaining backup tunnels with bandwidth protection. This is especially useful if you want to give LSPs carrying voice a higher priority than those carrying data.

To activate this feature, enter the `tunnel mpls traffic-eng fast-reroute bw-protect` command to set the “bandwidth protection desired” bit. See the Enabling Fast Reroute on LSPs, on page 17.

The LSPs do not necessarily receive bandwidth protection. They have a higher chance of receiving bandwidth protection if they need it.

LSPs that do not have the bandwidth protection bit set can be demoted. Demotion is when one or more LSPs are removed from their assigned backup tunnel to provide backup to an LSP that has its bandwidth protection bit set. Demotion occurs only when there is a scarcity of backup bandwidth.

When an LSP is demoted, it becomes unprotected (that is, it no longer has a backup tunnel). During the next periodic promotion cycle, an attempt is made to find the best possible backup tunnels for all LSPs that do not currently have protection, including the LSP that was demoted. The LSP may get protection at the same level or a lower level, or it may get no protection.

For information about how routers determine which LSPs to demote, see the Backup Bandwidth Protection, on page 7.

**RSVP Hello**

RSVP Hello enables a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational. This feature is useful when next-hop node failure is not detectable by link layer mechanisms,
or when notification of link-layer failures is not available (for example, Gigabit Ethernet). This allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

For a more detailed description of RSVP Hello, see the RSVP Hello, on page 5.

**Fast Reroute Operation**

This section describes the following:

**Fast Reroute Activation**

Two mechanisms cause routers to switch LSPs onto their backup tunnels:

- Interface down notification
- RSVP Hello neighbor down notification

When a router’s link or neighboring node fails, the router often detects this failure by an interface down notification. On a GSR Packet over SONET (PoS) interface, this notification is very fast. When a router notices that an interface has gone down, it switches LPSs going out that interface onto their respective backup tunnels (if any).

RSVP Hellos can also be used to trigger FRR. If RSVP Hellos are configured on an interface, messages are periodically sent to the neighboring router. If no response is received, Hellos declare that the neighbor is down. This causes any LSPs going out that interface to be switched to their respective backup tunnels.

**Backup Tunnels Terminating at Different Destinations**

The figure below illustrates an interface that has multiple backup tunnels terminating at different destinations and demonstrates why, in many topologies, support for node protection requires supporting multiple backup tunnels per protected interface.

*Figure 3: Backup Tunnels That Terminate at Different Destinations*

In this illustration, a single interface on R1 requires multiple backup tunnels. LSPs traverse the following routes:
To provide protection if node R2 fails, two NNHOP backup tunnels are required: one terminating at R3 and one terminating at R4.

**Backup Tunnels Terminating at the Same Destination**

The figure below shows how backup tunnels terminating at the same location can be used for redundancy and load balancing. Redundancy and load balancing work for both NHOP and NNHOP backup tunnels.

In this illustration, there are three routers: R1, R2, and R3. At R1 two NNHOP backup tunnels (T1 and T2) go from R1 to R3 without traversing R2.

Redundancy--If R2 fails or the link from R1 to R2 fails, either backup tunnel can be used. If one backup tunnel is down, the other can be used. LSPs are assigned to backup tunnels when the LSPs are first established. This is done before a failure.

Load balancing--If neither backup tunnel has enough bandwidth to back up all LSPs, both tunnels can be used. Some LSPs will use one backup tunnel, other LSPs will use the other backup tunnel. The router decides the best way to fit the LSPs onto the backup tunnels.

**Backup Tunnel Selection Procedure**

When an LSP is signaled, each node along the LSP path that provides FRR protection for the LSP selects a backup tunnel for the LSP to use if either of the following events occurs:

- The link to the next hop fails.
- The next hop fails.

By having the node select the backup tunnel for an LSP before a failure occurs, the LSP can be rerouted onto the backup tunnel quickly if there is a failure.

For an LSP to be mapped to a backup tunnel, all of the following conditions must exist:

- The LSP is protected by FRR; that is, the LSP is configured with the `tunnel mpls traffic-eng fast-reroute` command.
- The backup tunnel is up.
The backup tunnel is configured to have an IP address, typically a loopback address.

The backup tunnel is configured to protect this LSP’s outgoing interface; that is, the interface is configured with the `mpls traffic-eng backup-path` command.

The backup tunnel does not traverse the LSP’s protected interface.

The backup tunnel terminates at the LSP’s NHOP or NNHOP. If it is an NNHOP tunnel, it does not traverse the LSP’s NHOP.

The bandwidth protection requirements and constraints, if any, for the LSP and backup tunnel are met. For information about bandwidth protection considerations, see the Bandwidth Protection, on page 10.

### Bandwidth Protection

A backup tunnel can be configured to protect two types of backup bandwidth:

- **Limited backup bandwidth**—A backup tunnel provides bandwidth protection. The sum of the bandwidth of all LSPs using this backup tunnel cannot exceed the backup tunnel’s backup bandwidth. When you assign LSPs to this type of backup tunnel, sufficient backup bandwidth must exist.

- **Unlimited backup bandwidth**—The backup tunnel does not provide any bandwidth protection (that is, best-effort protection exists). There is no limit to the amount of bandwidth used by the LSPs that are mapped to this backup tunnel. LSPs that allocate zero bandwidth can use only backup tunnels that have unlimited backup bandwidth.

### Load Balancing on Limited-Bandwidth Backup Tunnels

There may be more than one backup tunnel that has sufficient backup bandwidth to protect a given LSP. In this case, the router chooses the one that has the least amount of backup bandwidth available. This algorithm limits fragmentation, maintaining the largest amount of backup bandwidth available.

Specifying limited backup bandwidth does not “guarantee” bandwidth protection if there is a link or node failure. For example, the set of NHOP and NNHOP backup tunnels that gets triggered when an interface fails may all share some link on the network topology, and this link may not have sufficient bandwidth to support all LSPs using this set of backup tunnels.
In the figure below, both backup tunnels traverse the same links and hop. When the link between routers R1 and R4 fails, backup tunnels for primary tunnel 1 and primary tunnel 2 are triggered simultaneously. The two backup tunnels may share a link in the network.

**Figure 4: Backup Tunnels Share a Link**

In the figure below, the backup tunnel for primary tunnel 1 may traverse routers R1-R2-R3-R4, and the backup tunnel for primary tunnel 2 may traverse routers R4-R2-R3-R1. In this case, the link R2-R3 may get overloaded if R1-R4 fails.

**Figure 5: Overloaded Link**

**Load Balancing on Unlimited-Bandwidth Backup Tunnels**

More than one backup tunnel, each having unlimited backup bandwidth, can protect a given interface. In this case, when choosing a backup tunnel for a given LSP, the router chooses the backup tunnel that has the least amount of backup bandwidth in use. This algorithm evenly distributes the LSPs across backup tunnels based on an LSP’s bandwidth. If an LSP is requesting zero bandwidth, the router chooses the backup tunnel that is protecting the fewest LSPs.
Pool Type and Backup Tunnels

By default, a backup tunnel provides protection for LSPs that allocate from any pool (that is, global or subpool). However, a backup tunnel can be configured to protect only LSPs that use global-pool bandwidth, or only those that use subpool bandwidth.

Tunnel Selection Priorities

This section describes the following:

NHOP Versus NNHOP Backup Tunnels

More than one backup tunnel can protect a given LSP, where one backup tunnel terminates at the LSP's NNHOP, and the other terminates at the LSP's NHOP. In this case, the router chooses the backup tunnel that terminates at the NNHOP (that is, FRR prefers NNHOP over NHOP backup tunnels).

The table below lists the tunnel selection priorities. The first choice is an NNHOP backup tunnel that acquires its bandwidth from a subpool or global pool, and has limited bandwidth. If there is no such backup tunnel, the next choice (2) is a next-nexthop backup tunnel that acquires a limited amount of bandwidth from any pool. The preferences go from 1 (best) to 8 (worst), where choice 3 is for an NNHOP backup tunnel with an unlimited amount of subpool or global-pool bandwidth.

Table 1: Tunnel Selection Priorities

<table>
<thead>
<tr>
<th>Preference</th>
<th>Backup Tunnel Destination</th>
<th>Bandwidth Pool</th>
<th>Bandwidth Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Best)</td>
<td>NNHOP</td>
<td>Subpool or global pool</td>
<td>Limited</td>
</tr>
<tr>
<td>2</td>
<td>NNHOP</td>
<td>Any</td>
<td>Limited</td>
</tr>
<tr>
<td>3</td>
<td>NNHOP</td>
<td>Subpool or global pool</td>
<td>Unlimited</td>
</tr>
<tr>
<td>4</td>
<td>NNHOP</td>
<td>Any</td>
<td>Unlimited</td>
</tr>
<tr>
<td>5</td>
<td>NHOP</td>
<td>Subpool or global pool</td>
<td>Limited</td>
</tr>
<tr>
<td>6</td>
<td>NHOP</td>
<td>Any</td>
<td>Limited</td>
</tr>
<tr>
<td>7</td>
<td>NHOP</td>
<td>Subpool or global pool</td>
<td>Unlimited</td>
</tr>
<tr>
<td>8 (Worst)</td>
<td>NHOP</td>
<td>Any</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

The figure below shows an example of the backup tunnel selection procedure based on the designated amount of global pool and subpool bandwidth currently available.
If NHOP and NNHOP backup tunnels do not have sufficient backup bandwidth, no consideration is given to the type of data that the LSP is carrying. For example, a voice LSP may not be protected unless it is signaled before a data LSP. To prioritize backup tunnel usage, see the "Backup Protection Preemption Algorithms" section.

**Figure 6: Choosing from Among Multiple Backup Tunnels**

In this example, an LSP requires 20 units (kilobits per second) of sub-pool backup bandwidth. The best backup tunnel is selected as follows:

1. Backup tunnels T1 through T4 are considered first because they terminate at the NNHOP.
2. Tunnel T4 is eliminated because it has only ten units of sub-pool backup bandwidth.
3. Tunnel T1 is eliminated because it protects only LSPs using global-pool bandwidth.
4. Tunnel T3 is chosen over T2 because, although both have sufficient backup bandwidth, T3 has the least backup bandwidth available (leaving the most backup bandwidth available on T2).
5. Tunnels T5 and T6 need not be considered because they terminate at an NHOP, and therefore are less desirable than T3, which terminates at an NNHOP.

**Promotion**

After a backup tunnel has been chosen for an LSP, conditions may change that will cause us to reevaluate this choice. This reevaluation, if successful, is called promotion. Such conditions may include:

1. A new backup tunnel comes up.
2. The currently chosen backup tunnel for this LSP goes down.
3. A backup tunnel’s available backup bandwidth increases. For example, an LSP protected by the tunnel has been reoptimized by the headend to use another path.
For cases 1 and 2, the LSP’s backup tunnel is evaluated immediately. Case 3 is addressed by periodically reevaluating LSP-to-backup tunnel mappings. By default, background reevaluation is performed every 5 minutes. This interval is configurable via the `mpls traffic-eng fast-reroute timers` command.

**Backup Protection Preemption Algorithms**

When you set the “bandwidth protection desired” bit for an LSP, the LSP has a higher right to select backup tunnels that provide bandwidth protection and it can preempt other LSPs that do not have that bit set.

If there is insufficient backup bandwidth on NNHOP backup tunnels but not on NHOP backup tunnels, the bandwidth-protected LSP does not preempt NNHOP LSPs; it uses NHOP protection.

If there are multiple LSPs using a given backup tunnel and one or more must be demoted to provide bandwidth, there are two user-configurable methods (algorithms) that the router can use to determine which LSPs are demoted:

- Minimize amount of bandwidth that is wasted.
- Minimize the number of LSPs that are demoted.

For example, If you need ten units of backup bandwidth on a backup tunnel, you can demote one of the following:

- A single LSP using 100 units of bandwidth--Makes available more bandwidth than needed, but results in lots of waste
- Ten LSPs, each using one unit of bandwidth--Results in no wasted bandwidth, but affects more LSPs

The default algorithm is to minimize the number of LSPs that are demoted. To change the algorithm to minimize the amount of bandwidth that is wasted, enter the `mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw` command.

**Bandwidth Protection Considerations**

There are numerous ways in which bandwidth protection can be ensured. The table below describes the advantages and disadvantages of three methods.

**Table 2: Bandwidth Protection Methods**

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve bandwidth for backup tunnels explicitly.</td>
<td>It is simple.</td>
<td>It is a challenge to allow bandwidth sharing of backup tunnels protecting against independent failures.</td>
</tr>
<tr>
<td>Use backup tunnels that are signaled with zero bandwidth.</td>
<td>It provides a way to share bandwidth used for protection against independent failures, so it ensures more economical bandwidth usage.</td>
<td>It may be complicated to determine the proper placement of zero bandwidth tunnels.</td>
</tr>
</tbody>
</table>
Cisco implementation of FRR does not mandate a particular approach, and it provides the flexibility to use any of the above approaches. However, given a range of configuration choices, be sure that the choices are constant with a particular bandwidth protection strategy.

The following sections describe some important issues in choosing an appropriate configuration:

**Using Backup Tunnels with Explicitly Signaled Bandwidth**

Two bandwidth parameters must be set for a backup tunnel:

- Actual signaled bandwidth
- Backup bandwidth

To signal bandwidth requirements of a backup tunnel, configure the bandwidth of the backup tunnel by using the `tunnel mpls traffic-eng bandwidth` command.

To configure the backup bandwidth of the backup tunnel, use the `tunnel mpls traffic-eng backup-bw` command.

The signaled bandwidth is used by the LSRs on the path of the backup tunnel to perform admission control and do appropriate bandwidth accounting.

The backup bandwidth is used by the point of local repair (PLR) (that is, the headend of the backup tunnel) to decide how much primary traffic can be rerouted to this backup tunnel if there is a failure.

Both parameters need to be set to ensure proper operation. The numerical value of the signaled bandwidth and the backup bandwidth should be the same.

**Protected Bandwidth Pools and the Bandwidth Pool from Which the Backup Tunnel Reserves Its Bandwidth**

The `tunnel mpls traffic-eng bandwidth` command allows you to configure the following:

- Amount of bandwidth a backup tunnel reserves
- The DS-TE bandwidth pool from which the bandwidth needs to be reserved

---

**Note**

Only one pool can be selected (that is, the backup tunnel can explicitly reserve bandwidth from either the global pool or the subpool, but not both).

The `tunnel mpls traffic-eng backup-bw` command allows you to specify the bandwidth pool to which the traffic must belong for the traffic to use this backup tunnel. Multiple pools are allowed.

There is no direct correspondence between the bandwidth pool that is protected and the bandwidth pool from which the bandwidth of the backup tunnel draws its bandwidth.
Bandwidth protection for 10 Kbps of subpool traffic on a given link can be achieved by configuring any of the following command combinations:

- `tunnel mpls traffic-eng bandwidth sub-pool 10`

- `tunnel mpls traffic-eng backup-bw sub-pool 10`
  - `tunnel mpls traffic-eng bandwidth global-pool 10`

- `tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool unlimited`
  - `tunnel mpls traffic-eng bandwidth global-pool 40`

- `tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool 30`

**Using Backup Tunnels Signaled with Zero Bandwidth**

Frequently it is desirable to use backup tunnels with zero signaled bandwidth, even when bandwidth protection is required. It may seem that if no bandwidth is explicitly reserved, no bandwidth guarantees can be provided. However, that is not necessarily true.

In the following situation:

- Only link protection is desired.
- Bandwidth protection is desired only for sub-pool traffic.

For each protected link AB with a maximum reservable subpool value of $n$, there may be a path from node A to node B such that the difference between the maximum reservable global and the maximum reservable subpool is at least the value of $n$. If it is possible to find such paths for each link in the network, you can establish all the backup tunnels along such paths without any bandwidth reservations. If there is a single link failure, only one backup tunnel will use any link on its path. Because that path has at least $n$ available bandwidth (in the global pool), assuming that marking and scheduling is configured to classify the subpool traffic into a priority queue, the subpool bandwidth is guaranteed.

This approach allows sharing of the global pool bandwidth between backup tunnels protecting independent link failures. The backup tunnels are expected to be used for only a short period of time after a failure (until the headends of affected LSPs reroute those LSPs to other paths with available subpool bandwidth). The probability of multiple unrelated link failures is very small (in the absence of node or shared risk link group (SRLG) failures, which result in multiple link failures). Therefore, it is reasonable to assume that link failures are in practice independent with high probability. This "independent failure assumption" in combination with backup tunnels signaled without explicit bandwidth reservation enables efficient bandwidth sharing that yields substantial bandwidth savings.

Backup tunnels protecting the subpool traffic do now draw bandwidth from any pool. Primary traffic using the global pool can use the entire global pool, and primary traffic using the subpool can use the entire subpool. Yet, subpool traffic has a complete bandwidth guarantee if there is a single link failure.

A similar approach can be used for node and SRLG protection. However, the decision of where to put the backup tunnels is more complicated because both node and SRLG failures effectively result in the simultaneous failure of several links. Therefore, the backup tunnels protecting traffic traversing all affected links cannot be computed independently of each other. The backup tunnels protecting groups of links corresponding to different failures can still be computed independently of each other, which results in similar bandwidth savings.
Signaled Bandwidth Versus Backup Bandwidth

Backup bandwidth is used locally (by the router that is the headend of the backup tunnel) to determine which, and how many, primary LSPs can be rerouted on a particular backup tunnel. The router ensures that the combined bandwidth requirement of these LSPs does not exceed the backup bandwidth.

Therefore, even when the backup tunnel is signaled with zero bandwidth, the backup bandwidth must be configured with the value corresponding to the actual bandwidth requirement of the traffic protected by this backup tunnel. Unlike the case when bandwidth requirements of the backup tunnels are explicitly signaled, the value of the signaled bandwidth (which is zero) is not the same value as the backup bandwidth.

How to Configure MPLS Traffic Engineering—Fast Reroute Link and Node Protection

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured.

Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if they have been configured as fast reroutable. To do this, enter the following commands at the headend of each LSP.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. tunnel mpls traffic-eng fast-reroute [bw-protect]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface tunnel number</td>
<td>Enters interface configuration mode for the specified tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface tunnel 1000</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

**Command or Action**

<table>
<thead>
<tr>
<th>Step 4</th>
<th>tunnel mpls traffic-eng fast-reroute [bw-protect]</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure.</td>
</tr>
</tbody>
</table>

### Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop

Creating a backup tunnel is basically no different from creating any other tunnel. To create a backup tunnel to the next hop or to the next-next hop, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the Finding Feature Information section.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** number
4. **ip unnumbered** interface-type interface-number
5. **tunnel destination** ip-address
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng path-option [protect] preference-number {dynamic | explicit {name path-name | path-number} } [lockdown]
8. **ip explicit-path name** word
9. **exclude-address** ip-address

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Command or Action</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Step 3</strong> interface tunnel <em>number</em></td>
<td>Creates a new tunnel interface and enters interface configuration mode. <strong>Example:</strong> Router(config)# interface tunnel 1</td>
</tr>
<tr>
<td><strong>Step 4</strong> ip unnumbered <em>interface-type interface-number</em></td>
<td>Gives the tunnel interface an IP address that is the same as that of interface Loopback0. <strong>Example:</strong> Router(config-if)# ip unnumbered loopback 0 <strong>Note</strong> This command is not effective until Loopback0 has been configured with an IP address.</td>
</tr>
<tr>
<td><strong>Step 5</strong> tunnel destination <em>ip-address</em></td>
<td>Specifies the IP address of the device where the tunnel will terminate. This address should be the router ID of the device that is the NHOP or NNHOP of LSPs to be protected. <strong>Example:</strong> Router(config-if)# tunnel destination 10.3.3.3</td>
</tr>
<tr>
<td><strong>Step 6</strong> tunnel mode mpls traffic-eng</td>
<td>Sets the encapsulation mode of the tunnel to MPLS TE. <strong>Example:</strong> Router(config-if)# tunnel mode mpls traffic-eng</td>
</tr>
<tr>
<td><strong>Step 7</strong> tunnel mpls traffic-eng path-option [protect] preference-number</td>
<td>Configures a path option for an MPLS TE tunnel. Enters router configuration mode. <strong>Example:</strong> Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit avoid-protected-link</td>
</tr>
<tr>
<td><strong>Step 8</strong> ip explicit-path name <em>word</em></td>
<td>Enters the command mode for IP explicit paths and creates the specified path. Enters explicit path command mode. <strong>Example:</strong> Router(config-router)# ip explicit-path name avoid-protected-link</td>
</tr>
<tr>
<td><strong>Step 9</strong> exclude-address <em>ip-address</em></td>
<td>For link protection, specify the IP address of the link to be protected. For node protection, specify the router ID of the node to be protected. <strong>Note</strong> Backup tunnel paths can be dynamic or explicit and they do not have to use exclude-address. Because backup tunnels must avoid the protected link or node, it is convenient to use the exclude-address command. <strong>Example:</strong></td>
</tr>
</tbody>
</table>
When using the `exclude-address` command to specify the path for a backup tunnel, you must exclude an interface IP address to avoid a link (for creating an NHOP backup tunnel), or a router ID address to avoid a node (for creating an NNHOP backup tunnel).

Example:

```
Router(config-ip-expl-path)# exclude-address 3.3.3.3
```

Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the Finding Feature Information section.

**Note** You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface type slot / port`
4. `mpls traffic-eng backup-path tunnel` `interface`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> <code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
Example: | • Enter your password if prompted.
Router> enable | 
Step 2 | configure terminal
Example: | Enters global configuration mode.
Router# configure terminal |
Step 3 | interface type slot / port
Example: | Moves configuration to the physical interface level, directing subsequent configuration commands to the specific physical interface identified by the type value. The slot and port identify the slot and port being configured. The interface must be a supported interface. See the Finding Feature Information section. Enters interface configuration mode.
Example: |
Example: |
Example: |
Example: |
Router(config)# interface POS 5/0 |
Step 4 | mpls traffic-eng backup-path tunnel interface
Example: | Allows LSPs going out this interface to use this backup tunnel if there is a link or node failure.
Router(config-if)# mpls traffic-eng backup-path tunnel 2 |
Note | You can enter this command multiple times to associate multiple backup tunnels with the same protected interface.

### Associating Backup Bandwidth and Pool Type with a Backup Tunnel

To associate backup bandwidth with a backup tunnel and designate the type of LSP that can use a backup tunnel, enter the following commands.
### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** `number`
4. **tunnel mpls traffic-eng backup-bw** `{bandwidth | [sub-pool {bandwidth | Unlimited}] [global-pool {bandwidth | Unlimited}]}

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** | enable | Enables privileged EXEC mode.  
- Enter your password if prompted.  

Example:  
Router> enable |
| **Step 2** | configure terminal | Enters global configuration mode.  

Example:  
Router# configure terminal |
| **Step 3** | interface tunnel `number` | Enters interface configuration mode for the specified tunnel.  

Example:  
Router(config)# interface tunnel 2 |
| **Step 4** | tunnel mpls traffic-eng backup-bw `{bandwidth | [sub-pool {bandwidth | Unlimited}] [global-pool {bandwidth | Unlimited}] |  

Example:  
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000 |

Associates bandwidth with a backup tunnel and designates whether LSPs that allocate bandwidth from the specified pool can use the tunnel.
# Configuring Backup Bandwidth Protection

## SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `tunnel mpls traffic-eng fast-reroute [bw-protect]`
4. `mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]`

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>enable</code></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Router&gt; enable</code></td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>2</td>
<td><code>configure terminal</code></td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>tunnel mpls traffic-eng fast-reroute [bw-protect]</code></td>
<td>Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect</code></td>
<td>The <code>bw-protect</code> keyword gives an LSP priority for using backup tunnels with bandwidth protection. Enters global configuration mode.</td>
</tr>
<tr>
<td>4</td>
<td><code>mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]</code></td>
<td>Changes the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw</code></td>
<td></td>
</tr>
</tbody>
</table>
Configuring an Interface for Fast Link and Node Failure Detection

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port
4. pos ais-shut
5. pos report \{b1-tca | b2-tca | b3-tca | lais | lrdd | pais | plop | prdd | rdool | sd-ber | sf-ber | slof | slos\}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router> enable | |
| Step 2 | configure terminal | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| Step 3 | interface type slot / port | Configures an interface type and enters interface configuration mode. |
| Example: | Router(config)# interface pos0/0 | |
| Step 4 | pos ais-shut | Sends the line alarm indication signal (LAIS) when the POS interface is placed in any administrative shutdown state. |
| Example: | Router(config-if)# pos ais-shut | |
| Step 5 | pos report \{b1-tca | b2-tca | b3-tca | lais | lrdd | pais | plop | prdd | rdool | sd-ber | sf-ber | slof | slos\} | Permits selected SONET alarms to be logged to the console for a POS interface. |
| Example: | Router(config-if)# pos report lrdd | |
Verifying That Fast Reroute Is Operational

To verify that FRR can function, perform the following task.

SUMMARY STEPS

1. show mpls traffic-eng tunnels brief
2. show ip rsvp sender detail
3. show mpls traffic-eng fast-reroute database
4. show mpls traffic-eng tunnels backup
5. show mpls traffic-eng fast-reroute database
6. show ip rsvp reservation

DETAILED STEPS

Step 1

show mpls traffic-eng tunnels brief

Use this command to verify that backup tunnels are up:

Example:

Router# show mpls traffic-eng tunnels brief

Signalling Summary:
LSPP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 1706 seconds

TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
Router_t1 10.112.0.12 - PO2/0/1 up/up
Router_t2 10.112.0.12 - unknown up/down
Router_t3 10.112.0.12 - unknown admin-down
Router_t1000 10.110.0.10 - unknown up/down
Router_t2000 10.110.0.10 - PO2/0/1 up/up

Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails

Step 2

show ip rsvp sender detail

Use this command to verify that LSPs are protected by the appropriate backup tunnels.

Following is sample output from the show ip rsvp sender detail command when the command is entered at the PLR before a failure:

Example:

Router# show ip rsvp sender detail

PATH:
Tun Dest: 10.10.0.6 Tun ID: 100 Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1 LSP ID: 31
Path refreshes:
arriving: from PHOP 10.10.7.1 on FE0/0/0 every 30000 msecs
Session Attr:
Setup Prio: 7, Holding Prio: 7
Flags: (0x7) Local Prot desired, Label Recording, SE Style
session Name: R1_t100
ERO: {incoming}
10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
10.10.7.1/32, Flags:0x0 (No Local Protection)
10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
Inbound FRR: Not active
Outbound FRR: No backup tunnel selected
Path ID handle: 50000416.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxy-terminated

Step 3
show mpls traffic-eng fast-reroute database
Enter the clear ip rsvp hello instance counters command to verify the following:

- MPLS TE FRR Node Protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

Example:

Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd AT2/0/0.100:Untagg Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 AT2/0/0.100:Pop ta Tu501:20 ready
10.0.8.9/24 Tu500 22 AT2/0/0.100:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the show mpls forwarding-table ip-address detail command. The final line of the display will tell whether that prefix is protected:

Example:

Router# show mpls forwarding-table 10.0.0.11 32 detail
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag swij or VC Tun hd or Tunnel Id switched interface
Untagged 10.0.0.11/32 48 pos1/0/0 point2point
MAC/Encaps=4/8, MTU=1520, Tag Stack(22)
4BD18847 00016000
No output feature configured
Fast Reroute Protection via (Tu0, outgoing label 12304)
The following command output displays the LSPs that are protected when the FRR primary tunnel is over an ATM interface and the backup tunnel is over a POS interface. As shown in the figure below, interface ATM2/0/0.100 is protected by backup tunnel 501.

**Figure 7: Protected LSPs**

![Diagram of LSPs](image)

This figure displays the protected LSPs:

- The primary tunnel is 500 and the path is R1 via ATM2/0/0.100 to R2, from R2 to R3, and from R3 to R4.
- The FRR backup tunnel is 501 and the path is R1 via POS0/2/0 to R2.
- The interface ATM2/0/0.100 is protected by the backup tunnel 501.

**Example:**

```bash
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd AT2/0/0.100:Untagg Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 AT2/0/0.100:Pop ta Tu501:20 ready
10.0.0.8/32 Tu500 19 AT2/0/0.100:Untagg Tu501:20 ready
10.8.9.0/24 Tu500 22 AT2/0/0.100:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

The following command output displays the LSPs that are protected when the FRR backup tunnel is over an ATM interface:

**Example:**

```bash
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel In-label Out intf/label FRR intf/label Status
Tunnel500 Tun hd PO0/2/0:Untagged Tu501:20 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32 Tu500 18 PO0/2/0:Pop tag Tu501:20 ready
10.0.0.8/32 Tu500 19 PO0/2/0:Untagg Tu501:20 ready
10.8.9.0/24 Tu500 22 PO0/2/0:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
```

**Step 4**

```bash
show mpls traffic-eng tunnels backup
```
The following conditions must exist for backup tunnels to be operational:

- **LSP is reroutable** -- At the headend of the LSP, enter the `show run int tunnel tunnel-number` command. The output should include the `tunnel mpls traffic-eng fast-reroute` command. If it does not, enter this command for the tunnel.

On the router where the backup tunnels originate, enter the `show mpls traffic-eng tunnels backup` command. Following is sample command output:

**Example:**
```
Router# show mpls traffic-eng tunnels backup
Router_t578
  LSP Head, Tunnel578, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.88.88.88, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0/0, PO1/1/0, PO0/3/3
    Backup BW: any pool unlimited; inuse: 100 kbps

Router_t5710
  LSP Head, Tunnel5710, Admin: admin-down, Oper: down
  Src 10.55.55.55, Dest 10.7.7.7, Instance 0
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/1/0
    Backup BW: any pool unlimited; inuse: 0 kbps

Router_t5711
  LSP Head, Tunnel5711, Admin: up, Oper: up
  Src 10.55.55.55, Dest 10.7.7.7, Instance 1
  Fast Reroute Backup Provided:
    Protected i/fs: PO1/0/0
    Protected lsps: 2
    Backup BW: any pool unlimited; inuse: 6010 kbps
```

The command output will allow you to verify the following:

- **Backup tunnel exists**--Verify that there is a backup tunnel that terminates at this LSP’s NHOP or NNHOP. Look for the LSP’s NHOP or NNHOP in the Dest field.

- **Backup tunnel is up**--To verify that the backup tunnel is up, look for "Up" in the State field.

- **Backup tunnel is associated with LSP’s I/F**--Verify that the interface for the LSP is allowed to use this backup tunnel. Look for the LSP’s output interface in the "protects" field list.

- **Backup tunnel has sufficient bandwidth**--If you restricted the amount of bandwidth a backup tunnel can hold, verify that the backup tunnel has sufficient bandwidth to hold the LSPs that would use this backup tunnel if there is a failure. The bandwidth of an LSP is defined by the line `tunnel mpls traffic-eng bandwidth` at the headend of the LSP. To determine the available bandwidth on a backup tunnel, look at the “cfg” and “inuse” fields. If there is insufficient backup bandwidth to accommodate the LSPs that would use this backup tunnel in the event of a failure, create an additional backup tunnel or increase the backup bandwidth of the existing tunnel by using the `tunnel mpls traffic-eng bandwidth` command.

**Note**

To determine how much bandwidth is sufficient, offline capacity planning may be required.

- **Backup tunnel has appropriate bandwidth type**--If you restricted the type of LSPs (subpool or global pool) that can use this backup tunnel, verify that the LSP is the appropriate type for the backup tunnel. The type of the LSP is defined by the line `tunnel mpls traffic-eng bandwidth` at the headend of this LSP. If this line contains the word "subpool", then it uses subpool bandwidth; otherwise, it uses global pool bandwidth. Verify that the type matches the type the backup tunnel can hold by looking in the output of the above command.
If none of the above actions works, enable debug by entering the `debug ip rsvp fast-reroute` command and the `debug mpls traffic-eng fast-reroute` command on the router that is the headend of the backup tunnel. Then do the following:

1. Enter the `shutdown` command for the primary tunnel.
2. Enter the `no shutdown` command for the primary tunnel.
3. View the debug output.

### Step 5

**show mpls traffic-eng fast-reroute database**

Enter the `clear ip rsvp hello instance counters` command to verify the following:

- MPLS TE FRR Node Protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

**Example:**

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel In-label intf/label FRR intf/label Status
Tunne110 Tun pos1/0/0:Untagged Tu0:12304 ready
Prefix item frr information:
Prefix Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.11/32 Tu110 Tun hd pos1/0/0:Untagged Tu0:12304 ready
LSP midpoint frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
10.0.0.12 1 [459] 16 pos0/1/0:17 Tu2000:19 ready
```

**Note**

If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the `show mpls forwarding-table ip-address detail` command. The final line of the display will tell whether that prefix is protected:

**Example:**

```
Router# show mpls forwarding-table 10.0.0.11 32 detail
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
Tun hd Untagged 10.0.0.11/32 48 pos0/0/0:17 point2point
MAC/Encaps=4/8, MTU=1520, Tag Stack(22)
48D18847 00016000
No output feature configured
Fast Reroute Protection via (Tu0, outgoing label 12304)
```

### Step 6

**show ip rsvp reservation**

Following is sample output from the `show ip rsvp reservation` command entered at the headend of a primary LSP. Entering the command at the head-end of the primary LSP shows, among other things, the status of FRR (that is, local protection) at each hop this LSP traverses. The per-hop information is collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

**Example:**

```
Router# show ip rsvp reservation detail
```

Reservation:
Tun Dest: 10.1.1.1  Tun ID: 1  Ext Tun ID: 10.1.1.1
Tun Sender: 10.1.1.1  LSP ID: 104
Next Hop: 10.1.1.2 on POS1/0/0
Label: 18 (outgoing)
Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
Average Bitrate is 0 bits/sec, Maximum Burst is 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
RRO:
  10.1.1.1/32, Flags:0x1 (Local Prot Avail/to NHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 18
  10.1.1.1/32, Flags:0x0 (Local Prot Avail/In Use/Has BW/to NHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 16
  10.1.1.2/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 0
Resv ID handle: CD000404.
Policy: Accepted. Policy source(s): MPLS/TE

Notice the following about the primary LSP:

- It has protection that uses a NHOP backup tunnel at its first hop.
- It has protection and is actively using an NHOP backup tunnel at its second hop.
- It has no local protection at its third hop.

The RRO display shows the following information for each hop:

- Whether local protection is available (that is, whether the LSP has selected a backup tunnel)
- Whether local protection is in use (that is, whether the LSP is currently using its selected backup tunnel)
- Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel
- Whether the backup tunnel used at this hop provides bandwidth protection

Troubleshooting Tips

This section describes the following:

LSPs Do Not Become Active; They Remain Ready

At a PLR, LSPs transition from Ready to Active if one of the following events occurs:

- Primary interface goes down--If the primary interface (LSP’s outbound interface) goes down and the LSP is ready to use a backup tunnel, the LSP will transition to the active state causing its data to flow over the backup tunnel. On some platforms and interface types (for example, GSR POS interfaces), there is fast interface-down logic that detects this event very quickly. On other platforms where this logic does not exist, detection time is slower. On such platforms, it may be desirable to enable RSVP Hello (see the next bulleted item, “Hellos detect next hop is down”).

- Hellos detect next hop is down--If Hellos are enabled on the primary interface (LSP’s outbound interface), and the LSP’s next hop is no longer reachable, the next hop is declared down. This event will cause the LSP to begin actively using its backup tunnel. Notice that a next hop will be declared down even if the primary interface does not go down. For example, if the next hop stops responding due to a reboot or software or hardware problem, Hellos will trigger the LSPs using this next hop to switch to their backup...
tunnels. Hellos can also help trigger FRR on interfaces such as Gigabit Ethernet where the interface remains up but is unusable (due to lack of link-layer liveness detection mechanisms).

**Primary Tunnel Does Not Select Backup Tunnel That Is Up**
If a backup tunnel is up, but it is not selected as a backup tunnel by the primary tunnel (LSP), enter the following commands for the backup tunnel:

- `shutdown`
- `no shutdown`

**Note**
If you change the status of a backup tunnel, the backup tunnel selection algorithm is rerun for the backup tunnel. LSPs that have currently selected (that is, are ready to use) that backup tunnel will be disassociated from it, and then reassociated with that backup tunnel or another backup tunnel. This is generally harmless and usually results in mapping the same LSPs to that backup tunnel. However, if any LSPs are actively using that backup tunnel, shutting down the backup tunnel will tear down those LSPs.

**Enhanced RSVP Commands Display Useful Information**
The following RSVP commands have been enhanced to display information that can be helpful when you are examining the FRR state or troubleshooting FRR:

- `show ip rsvp request` -- Displays upstream reservation state (that is, information related to the Resv messages that this node will send upstream).
- `show ip rsvp reservation` -- Displays information about Resv messages received.
- `show ip rsvp sender` -- Displays information about path messages being received.

These commands show control plane state; they do not show data state. That is, they show information about RSVP messages (Path and Resv) used to signal LSPs. For information about the data packets being forwarded along LSPs, use the `show mpls forwarding` command.

**RSVP Hello Detects When a Neighboring Node Is Not Reachable**
The RSVP Hello feature enables RSVP nodes to detect when a neighboring node is not reachable. Use this feature when notification of link-layer failures is not available and unnumbered links are not used, or when the failure detection mechanisms provided by the link layer are not sufficient for timely node failure detection. Hello must be configured both globally on the router and on the specific interface to be operational.

**Hello Instances Have Not Been Created**
If Hello instances have not been created, do the following:

- Determine if RSVP Hello has been enabled globally on the router. Enter the `ip rsvp signalling hello`(configuration) command.
- Determine if RSVP Hello has been enabled on an interface that the LSPs traverse. Enter the `ip rsvp signalling hello`(interface) command.
- Verify that at least one LSP has a backup tunnel by displaying the output of the `show ip rsvp sender` command. A value of ”Ready” indicates that a backup tunnel has been selected.
“No entry at index” (error may self-correct, RRO may not yet have propagated from downstream node of interest) Error Message Is Printed at the Point of Local Repair

FRR relies on a RRO in Resv messages arriving from downstream. Routers receiving path messages with the SESSION_ATTRIBUTE bit indicating that the LSP is fast-reroutable should include an RRO in the corresponding Resv messages.

If an LSP is configured for FRR, but the Resv arriving from a downstream router contains an incomplete RRO, the "No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)” message is printed. An incomplete RRO is one in which the NHOP or the NNHOP did not include an entry in the RRO.

This error typically means that backup tunnels to the NHOP or the NNHOP cannot be selected for this LSP because there is insufficient information about the NHOP or NNHOP due to the lack of an RRO entry.

Occasionally there are valid circumstances in which this situation occurs temporarily and the problem is self-corrected. If subsequent Resv messages arrive with a complete RRO, ignore the error message.

To determine whether the error has been corrected, display the RRO in Resv messages by entering the **clear ip rsvp hello instance counters** command. Use an output filter keyword to display only the LSP of interest.

“Couldn’t get rsbs” (error may self-correct when Resv arrives) Error Message Is Printed at the Point of Local Repair

The PLR cannot select a backup tunnel for an LSP until a Resv message has arrived from downstream.

When this error occurs, it typically means that something is wrong. For example, no reservation exists for this LSP. You can troubleshoot this problem by using the **debug ip rsvp reservation** command to enable debug.

Occasionally there are valid circumstances in which this error message occurs and there is no need for concern. One such circumstance is when an LSP experiences a change before any Resv message has arrived from downstream. Changes can cause a PLR to try to select a backup tunnel for an LSP, and the selection will fail (causing this error message) if no Resv message has arrived for this LSP.
Configuration Examples for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

The examples relate to the illustration shown in the figure below.

![Backup Tunnels Diagram]

**Figure 8: Backup Tunnels**

**Enabling Fast Reroute for all Tunnels Example**

On router R1, enter interface configuration mode for each tunnel to be protected (Tunnel 1000 and Tunnel 2000). Enable these tunnels to use a backup tunnel in case of a link or node failure along their paths.

Tunnel 1000 will use 10 units of bandwidth from the subpool.

Tunnel 2000 will use five units of bandwidth from the global pool. The "bandwidth protection desired" bit has been set by specifying `bw-prot` in the `tunnel mpls traffic-eng fast-reroute` command.

```
Router(config)# interface Tunnel 1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```

**Creating an NHOP Backup Tunnel Example**

On router R2, create an NHOP backup tunnel to R3. This backup tunnel should avoid using the link 172.1.1.2.

```
Router(config)# ip explicit-path name avoid-protected-link
Router(config-if)# exclude-address 172.1.1.2
```
Creating an NNHOP Backup Tunnel Example

On router R2, create an NNHOP backup tunnel to R4. This backup tunnel should avoid R3.

```
Router(config)# ip explicit-path name avoid-protected-node
Router(cfg-ip-expl-path)# exclude-address 10.3.3.3
```

Assigning Backup Tunnels to a Protected Interface Example

On router R2, associate both backup tunnels with interface POS 5/0:

```
Router(config)# interface POS 5/0
Router(config-if)# mpls traffic-eng backup-path tunnel 1
Router(config-if)# mpls traffic-eng backup-path tunnel 2
```

Associating Backup Bandwidth and Pool Type with Backup Tunnels Example

Backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. It does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

```
Router(config)# interface Tunnel 1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config)# interface Tunnel 2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000
```
Configuring Backup Bandwidth Protection Example

In the following example, backup bandwidth protection is configured:

This global configuration is required only to change the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw
```

Configuring an Interface for Fast Link and Node Failure Detection Example

In the following example, pos ais-shut is configured:

```
Router(config)# interface pos 0/0
Router(config-if)# pos ais-shut
```

In the following example, report lrdi is configured on OS interfaces:

```
Router(config)# interface pos 0/0
Router(config-if)# pos report lrdi
```

Configuring RSVP Hello and POS Signals Example

Hello must be configured both globally on the router and on the specific interface on which you need FRR protection. To configure Hello, use the following configuration commands:

- `ip rsvp signalling hello` (configuration)--Enables Hello globally on the router.
- `ip rsvp signalling hello` (interface)--Enables Hello on an interface where you need FRR protection.

The following configuration commands are optional:

- `ip rsvp signalling hello dscp` --Sets the differentiated services code point (DSCP) value that is in the IP header of the Hello message.
- `ip rsvp signalling hello refresh misses` --Specifies how many acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
- `ip rsvp signalling hello refresh interval` --Configures the Hello request interval.
- `ip rsvp signalling hello statistics` --Enables Hello statistics on the router.

For configuration examples, see the Hello command descriptions in the "Command Reference" section of `MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support`, Release 12.0(24)S.

To configure POS signaling for detecting FRR failures, enter the `pos report all` command or enter the following commands to request individual reports:

```
pos ais-shut
```
## Additional References

### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS</td>
<td><em>Cisco IOS IP Routing Protocols Command Reference</em></td>
</tr>
<tr>
<td></td>
<td>Configuring a Basic IS-IS Network</td>
</tr>
<tr>
<td>Link protection</td>
<td>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</td>
</tr>
<tr>
<td>Shared risk link groups</td>
<td>MPLS Traffic Engineering: Shared Risk Link Groups</td>
</tr>
<tr>
<td></td>
<td>MPLS Traffic Engineering: Inter-AS TE</td>
</tr>
<tr>
<td>FRR protection of TE LSPs from SRLG failure</td>
<td>MPLS Traffic Engineering: Shared Risk Link Groups</td>
</tr>
<tr>
<td>MPLS traffic engineering commands</td>
<td><em>Cisco IOS Multiprotocol Label Switching Command Reference</em></td>
</tr>
<tr>
<td>Configuration of MPLS TE tunnels</td>
<td>MPLS Traffic Engineering: Interarea Tunnels</td>
</tr>
<tr>
<td>OSPF</td>
<td><em>Cisco IOS IP Routing Protocols Command Reference</em></td>
</tr>
<tr>
<td></td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>RSVP</td>
<td><em>Cisco IOS Quality of Service Solutions Command Reference</em></td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-mpls-rsvp-lsp-fastreroute-04.txt</td>
<td>Fast ReRoute Extensions to RSVP-TE for LSP Tunnels</td>
</tr>
</tbody>
</table>
MIBs

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

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>

Command Reference


- clear ip rsvp hello instance counters
- clear ip rsvp hello instance statistics
• clear ip rsvp hello statistics
• debug ip rsvp hello
• ip rsvp signalling hello (configuration)
• ip rsvp signalling hello (interface)
• ip rsvp signalling hello dscp
• ip rsvp signalling hello refresh interval
• ip rsvp signalling hello refresh misses
• ip rsvp signalling hello statistics
• mpls traffic-eng backup-path tunnel
• mpls traffic-eng fast-reroute backup-prot-preemption
• mpls traffic-eng fast-reroute timers
• show ip rsvp fast bw-protect
• show ip rsvp fast detail
• show ip rsvp hello
• show ip rsvp hello instance detail
• show ip rsvp hello instance summary
• show ip rsvp hello statistics
• show ip rsvp interface detail
• show ip rsvp request
• show ip rsvp reservation
• show ip rsvp sender
• show mpls traffic tunnel backup
• show mpls traffic-eng fast-reroute database
• show mpls traffic-eng tunnels
• show mpls traffic-eng tunnels summary
• tunnel mpls traffic-eng backup-bw
• tunnel mpls traffic-eng fast-reroute

Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 3: Feature Information for MPLS Traffic Engineering—Fast Reroute Link and Node Protection**

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Traffic Engineering--Fast Reroute Link and Node Protection</td>
<td></td>
<td>The MPLS Traffic Engineering--Fast Reroute Link and Node Protection feature supports link protection (backup tunnels that bypass only a single link of the label-switched path (LSP)), node protection (backup tunnels that bypass next-hop nodes along LSPs), and the following FRR features: backup tunnel support, backup bandwidth protection, and RSVP Hellos.</td>
</tr>
</tbody>
</table>
Feature Information

Releases

Feature Name

The following commands were introduced or modified:
clear ip rsvp hello instance counters,
clear ip rsvp hello instance statistics, clear ip rsvp hello statistics, debug ip rsvp hello, ip rsvp signalling hello (configuration), ip rsvp signalling hello (interface), ip rsvp signalling hello dscp, ip rsvp signalling hello refresh interval, ip rsvp signalling hello refresh misses, ip rsvp signalling hello statistics, mpls traffic-eng backup-path tunnel, mpls traffic-eng fast-reroute backup-prot-preemption, mpls traffic-eng fast-reroute timers, show ip rsvp fast bw-protect, show ip rsvp fast detail, show ip rsvp hello, show ip rsvp hello instance detailed, show ip rsvp hello instance summary, show ip rsvp hello statistics, show ip rsvp interface detail, show ip rsvp request, show ip rsvp reservation, show ip rsvp sender, show mpls traffic tunnel backup, show mpls traffic-eng fast-reroute database, show mpls traffic-eng tunnels, show mpls traffic-eng tunnels summary, tunnel mpls traffic-eng backup-bw, tunnel mpls traffic-eng fast-reroute.

Glossary

**backup bandwidth** --The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

**backup tunnel** --An MPLS TE tunnel used to protect other (primary) tunnels’ traffic when a link or node failure occurs.

**bandwidth** --The available traffic capacity of a link.
Cisco Express Forwarding -- A means for accelerating the forwarding of packets within a router, by storing route lookup.

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

Fast Reroute -- Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

global pool -- The total bandwidth allocated to an MPLS traffic engineering link or node.

headend -- The router that originates and maintains a given LSP. This is the first router in the LSP's path.

hop -- Passage of a data packet between two network nodes (for example, between two routers).

instance -- A Hello instance implements the RSVP Hello extensions for a given router interface address and remote IP address. Active Hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

interface -- A network connection.

Intermediate System-to-Intermediate System -- IS-IS. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

link -- A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

limited backup bandwidth -- Backup tunnels that provide bandwidth protection.

load balancing -- A configuration technique that shifts traffic to an alternative link if a certain threshold is exceeded on the primary link. Load balancing is similar to redundancy in that if an event causes traffic to shift directions, alternative equipment must be present in the configuration. In load balancing, the alternative equipment is not necessarily redundant equipment that operates only in the event of a failure.

LSP -- label-switched path. A connection between two routers in which MPLS forwards the packets.

merge point -- The backup tunnel's tail.

MPLS -- Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

MPLS global label allocation -- There is one label space for all interfaces in the router. For example, label 100 coming in one interface is treated the same as label 100 coming in a different interface.

NHOP -- next hop. The next downstream node along an LSP's path.

NHOP backup tunnel -- next-hop backup tunnel. Backup tunnel terminating at the LSP's next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

NNHOP -- next-next hop. The node after the next downstream node along an LSP's path.

NNHOP backup tunnel -- next-next-hop backup tunnel. Backup tunnel terminating at the LSP's next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.
**node** -- Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.

**OSPF** -- Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**primary LSP** -- The last LSP originally signaled over the protected interface before the failure. The primary LSP is the LSP before the failure.

**primary tunnel** -- Tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**promotion** -- Conditions, such as a new backup tunnel comes up, cause a reevaluation of a backup tunnel that was chosen for an LSP. If the reevaluation is successful, it is called a promotion.

**protected interface** -- An interface that has one or more backup tunnels associated with it.

**redundancy** -- The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

**RSVP** -- Resource Reservation Protocol. A protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

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

**SRLG** -- shared risk link group. Sets of links that are likely to go down together.

**state** -- Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**sub-pool** -- The more restrictive bandwidth in an MPLS traffic engineering link or node. The subpool is a portion of the link or node’s overall global pool bandwidth.

**tailend** -- The router upon which an LSP is terminated. This is the last router in the LSP’s path.

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

**tunnel** -- Secure communications path between two peers, such as two routers.

**unlimited backup bandwidth** -- Backup tunnels that provide no bandwidth (best-effort) protection (that is, they provide best-effort protection).
CHAPTER 2

MPLS TE Link and Node Protection with RSVP Hellos Support

The MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) feature provides the following Fast Reroute (FRR) capabilities:

• Backup tunnel that terminates at the next-next hop router to protect both the downstream link and node in order to protect link and node failures. There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. A backup tunnel is scalable because it can protect multiple label switched paths (LSPs) and multiple interfaces.

• Backup bandwidth protection allows a priority to be assigned to backup tunnels for LSPs carrying certain kinds of data (such as voice).

• Fast Tunnel Interface Down detection, which forces a "generic" interface tunnel (not specifically a Fast Reroute tunnel) to become disabled immediately if the headend router detects a failed link on an LSP.

• Resource Reservation Protocol (RSVP) Hellos, which are used to accelerate the detection of node failures.

Note

If the Multiprotocol Label Switching (MPLS) TE FRR Link Protection feature is planned to be used in releases earlier than Cisco IOS Release 12.0(24)S, contact the Cisco Technical Assistance Center for important deployment and upgrade information.

For information about shared risk link groups (SRLGs), which are sets of links that are likely to go down together, refer to MPLS Traffic Engineering: Shared Risk Link Groups.

• Finding Feature Information, page 44
• Prerequisites for MPLS TE Link and Node Protection with RSVP Hellos Support, page 44
• Restrictions for MPLS TE Link and Node Protection with RSVP Hellos Support, page 44
• Information About MPLS TE Link and Node Protection with RSVP Hellos Support, page 45
• How to Configure MPLS TE Link and Node Protection with RSVP Hellos Support, page 60
• Config Examples for MPLS TE Link and Node Protection with RSVP Hellos Support, page 77
• Additional References, page 80
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 Link and Node Protection with RSVP Hellos Support

Your network must support the following Cisco IOS features in order to support features described in this document:

- IP Cisco Express Forwarding
- MPLS

Your network must support at least one of the following protocols:

- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)

Restrictions for MPLS TE Link and Node Protection with RSVP Hellos Support

- Interfaces must use MPLS Global Label Allocation.
- Backup tunnel headend and tailend routers must implement FRR as described in this document.
- Backup tunnels are not protected. If an LSP is actively using a backup tunnel and the backup tunnel fails, the LSP is torn down.
- LSPs that are actively using backup tunnels are not considered for promotion. So, if an LSP is actively using a backup tunnel and a better backup tunnel becomes available, the active LSP is not switched to the better backup tunnel.
Information About MPLS TE Link and Node Protection with RSVP Hellos Support

Fast Reroute

MPLS Fast Reroute (FRR) is a fast recovery local protection technique that protects TE LSPs from link, shared risk link group (SRLG), and node failure. One or more TE LSPs (called backup LSPs) are preestablished to protect against the failure of a link, node, or SRLG. If there is a failure, each protected TE LSP traversing the failed resource is rerouted onto the appropriate backup tunnels.

The backup tunnel must meet the following requirements:

- It should not pass through the element it protects.
- It should intersect with a primary tunnel at a minimum of two nodes: point of local repair (PLR) and merge point (MP). The PLR should be the headend LSR of the backup tunnel, and the MP should be the tailend LSR of the backup tunnel. The PLR is where FRR is triggered when a link, node, or SRLG failure occurs.
- FRR protection can be performed for an Inter-AS tunnel only if the backup tunnel's merge point can route packets to the PLR's backup tunnel's egress interface. You can configure a static route or you can configure Border Gateway Protocol (BGP) to export the backup tunnel's egress interface to other autonomous systems.
- If the preferred link is a passive link, you must assign an administrative-weight for it. To assign an administrative weight, use the `mpls traffic-eng administrative-weight` command in interface configuration mode.
- Each router must be configured with the `mpls traffic-eng reoptimize events link-up` command in global configuration mode.

Link Protection

Backup tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP's next hop beyond the point of failure.

Node Protection

FRR provides Node Protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of RSVP Hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link in addition to the node.
The figure below illustrates an NNHOP backup tunnel.

*Figure 9: NNHOP Backup Tunnel*

If an LSP is using a backup tunnel and something changes so that the LSP is no longer appropriate for the backup tunnel, the LSP is torn down. Such changes include the following:

- Backup bandwidth of the backup tunnel is reduced.
- Backup bandwidth type of backup tunnel is changed to a type that is incompatible with the primary LSP.
- Primary LSP is modified so that FRR is disabled. (The `no mpls traffic-eng fast-reroute` command is entered.)

**Bandwidth Protection**

NHOP and NNHOP backup tunnels can be used to provide bandwidth protection for rerouted LSPs. This is referred to as backup bandwidth. You can associate backup bandwidth with NHOP or NNHOP backup tunnels. This informs the router of the amount of backup bandwidth a particular backup tunnel can protect. When a router maps LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given backup tunnel only if there is sufficient backup bandwidth. The router selects which LSPs use which backup tunnels in order to provide maximum bandwidth protection. That is, the router determines the best way to map LSPs onto backup tunnels in order to maximize the number of LSPs that can be protected. For information about mapping tunnels and assigning backup bandwidth, see the "Backup Tunnel Selection Procedure" section.

LSPs that have the "bandwidth protection desired" bit set have a higher right to select backup tunnels that provide bandwidth protection; that is, those LSPs can preempt other LSPs that do not have that bit set. For more information, see the "Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection" section.
Fast Tunnel Interface Down Detection

Fast Tunnel Interface Down detection forces a "generic" interface tunnel (not specifically a Fast Reroute tunnel) to become disabled immediately if the headend router detects a failed link on an LSP.

This feature is configured with the `tunnel mpls traffic-eng interface down delay` command. If this feature is not configured, there is a delay before the tunnel becomes unoperational and before the traffic uses an alternative path chosen by the headend/midpoint router to forward the traffic. This is acceptable for data traffic, but not for voice traffic because it relies on the TE tunnel to go down as soon as the LSP goes down.

RSVP Hello

RSVP Hello enables a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational. This feature is useful when next-hop node failure is not detectable by link layer mechanisms, or when notification of link-layer failures is not available. This allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

For a more detailed description of RSVP Hello, see the RSVP Hello.

RSVP Hello Operation

RSVP Hello enables RSVP nodes to detect when a neighboring node is not reachable. This provides node-to-node failure detection. When such a failure is detected, it is handled in a similar manner as a link-layer communication failure.

RSVP Hello can be used by FRR when notification of link-layer failures is not available (for example, with Ethernet), or when the failure detection mechanisms provided by the link layer are not sufficient for the timely detection of node failures.

A node running Hello sends a Hello Request to a neighboring node every interval. If the receiving node is running Hello, it responds with Hello Ack. If four intervals pass and the sending node has not received an Ack or it receives a bad message, the sending node declares that the neighbor is down and notifies FRR.

There are two configurable parameters:

- Hello interval, by using the `ip rsvp signalling hello refresh interval` command
- Number of acknowledgment messages that are missed before the sending node declares that the neighbor is down, by using the `ip rsvp signalling hello refresh misses` command

Note

If a router’s CPU utilization is high due to frequent RSVP Hello processing, there may be false failures due to Hello messages that are not transmitted.

Hello Instance

A Hello instance implements RSVP Hello for a given router interface address and 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, create a Hello instance only when it is necessary and delete it when it is no longer needed.
There are two types of Hello instances:

- Hello Instance, on page 47
- Hello Instance, on page 47

**Active Hello Instances**

If a neighbor is unreachable when an LSP is ready to be fast rerouted, an active Hello instance is needed. Create an active Hello instance for each neighbor with at least one LSP in this state.

Active Hello instances periodically send Hello Request messages, and expect Hello Ack messages in response. If the expected Ack message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (lost). LSPs traversing that neighbor may be fast rerouted.

If there is a Hello instance with no LSPs for an unreachable neighbor, do not delete the Hello instance. Convert the active Hello instance to a passive Hello instance because there may be an active instance on the neighboring router that is sending Hello requests to this instance.

**Passive Hello Instances**

Passive Hello instances respond to Hello Request messages (sending Ack messages), but do not initiate Hello Request messages and do not cause LSPs to be fast rerouted. A router with multiple interfaces can run multiple Hello instances to different neighbors or to the same neighbor.

A passive Hello instance is created when a Hello Request is received from a neighbor with a source IP address/destination IP address pair in the IP header for which a Hello instance does not exist.

Delete passive instances if no Hello messages are received for this instance within 10 minutes.

**Hello Commands**

RSVP Hello comprises the following commands. For detailed command descriptions, refer to MPLS Traffic Engineering--RSVP Hello State Timer.

- RSVP Hello Configuration Commands
- RSVP Hello Statistics Commands
- RSVP Hello Show Commands
- RSVP Hello Debug Commands

**Features of MPLS TE Link and Node Protection with RSVP Hellos Support**

MPLS TE Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) includes the following features:

**Backup Tunnel Support**

Backup tunnel support has the following capabilities:
Backup Tunnels Can Terminate at the Next-Next Hop to Support FRR

Backup tunnel that terminates at the next-next hop router to protect both the downstream link and node in order to protect link and node failures. For more detailed information, see the Node Protection, on page 45.

Multiple Backup Tunnels Can Protect the Same Interface

There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. In many topologies, support for Node Protection requires supporting multiple backup tunnels per protected interface. These backup tunnels can terminate at the same destination or at different destinations. That is, for a given protected interface, you can configure multiple NHOP or NNHOP backup tunnels. This allows redundancy and load balancing.

In addition to being required for Node Protection, this feature provides the following benefits:

- Redundancy--If one backup tunnel is down, other backup tunnels protect LSPs.
- Increased backup capacity--If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels). For a more detailed explanation, see the Backup Tunnel Selection Procedure, on page 52.

Examples are shown in the Backup Tunnels Terminating at Different Destinations, on page 51 and the Backup Tunnels Terminating at the Same Destination, on page 52.

Scalability

A backup tunnel is scalable because it can protect multiple LSPs and multiple interfaces. It provides many-to-one (N:1) protection, which has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

Example of 1:1 protection: When 5,000 backup tunnels protect 5,000 LSPs, each router along the backup path must maintain state for an additional 5,000 tunnels.

Example of N:1 protection: When one backup tunnel protects 5,000 LSPs, each router along the backup path maintains one additional tunnel.

Backup Bandwidth Protection

Backup bandwidth protection has the following capabilities:

Bandwidth Protection on Backup Tunnels

Rerouted LSPs not only have their packets delivered during a failure, but the quality of service can also be maintained.

Bandwidth Pool Specifications for Backup Tunnels

You can restrict the types of LSPs that can use a given backup tunnel. Backup tunnels can be restricted so that only LSPs using subpool bandwidth can use them or only LSPs that use global pool bandwidth can use them. This allows different backup tunnels to be used for voice and data. Example: The backup tunnel used for voice could provide bandwidth protection, and the backup tunnel used for data could (optionally) not provide bandwidth protection.
**Semidynamic Backup Tunnel Paths**

The path of a backup tunnel can be configured to be determined dynamically. This can be done by using the IP explicit address exclusion feature that was added in Release 12.0(14)ST. Using this feature, semidynamic NHOP backup tunnel paths can be specified simply by excluding the protected link; semidynamic NNHOP backup tunnel paths can be configured simply by excluding the protected node.

**Prioritizing Which LSPs Obtain Backup Tunnels with Bandwidth Protection**

In case there are not enough NHOP or NNHOP backup tunnels or they do not have enough backup bandwidth to protect all LSPs, you can give an LSP priority in obtaining backup tunnels with bandwidth protection. This is especially useful if you want to give LSPs carrying voice a higher priority than those carrying data.

To activate this feature, enter the `tunnel mpls traffic-eng fast-reroute bw-protect` command to set the “bandwidth protection desired” bit. See the configuration task Enabling Fast Reroute on LSPs. The LSPs do not necessarily receive bandwidth protection. They have a higher chance of receiving bandwidth protection if they need it.

LSPs that do not have the bandwidth protection bit set can be demoted. Demotion is when one or more LSPs are removed from their assigned backup tunnel to provide backup to an LSP that has its bandwidth protection bit set. Demotion occurs only when there is a scarcity of backup bandwidth.

When an LSP is demoted, it becomes unprotected (that is, it no longer has a backup tunnel). During the next periodic promotion cycle, an attempt is made to find the best possible backup tunnels for all LSPs that do not currently have protection, including the LSP that was demoted. The LSP may get protection at the same level or a lower level, or it may get no protection.

For information about how routers determine which LSPs to demote, see the "Backup Protection Preemption Algorithms" section.

**RSVP Hello**

RSVP Hello enables a router to detect when a neighboring node has gone down but its interface to that neighbor is still operational. This feature is useful when next-hop node failure is not detectable by link layer mechanisms, or when notification of link-layer failures is not available (for example, Gigabit Ethernet). This allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

For a more detailed description of RSVP Hello, see the RSVP Hello Operation.

**Fast Reroute Operation**

This section describes the following:

**Fast Reroute Activation**

Three mechanisms cause routers to switch LSPs onto their backup tunnels:

- Interface down notification
- Loss of Signal
- RSVP Hello neighbor down notification
When a router’s link or neighboring node fails, the router often detects this failure by an interface down notification. On a Packet over SONET (POS) interface, this notification is very fast. When a router notices that an interface has gone down, it switches LPSs going out that interface onto their respective backup tunnels (if any).

Unlike POS interfaces, Gigabit Ethernet does not have any alarms to detect link failures. If a link is down due to a cut cable or because the remote end shuts its laser, the optics module (GBIC or SFPs) on the Gigabit Ethernet card detects a loss of signal (LOS). The LOS is used as a mechanism to detect the failure and begin the switchover.

RSVP Hellos can also be used to trigger FRR. If RSVP Hellos are configured on an interface, messages are periodically sent to the neighboring router. If no response is received, Hellos declare that the neighbor is down. This causes any LSPs going out that interface to be switched to their respective backup tunnels.

Fast Reroute also works over ATM interfaces. The interfaces must use RSVP Hello to detect failures.

**Backup Tunnels Terminating at Different Destinations**

The figure below illustrates an interface that has multiple backup tunnels terminating at different destinations and demonstrates why, in many topologies, support for Node Protection requires supporting multiple backup tunnels per protected interface.

*Figure 10: Backup Tunnels that Terminate at Different Destinations*

In this illustration, a single interface on R1 requires multiple backup tunnels. LSPs traverse the following routes:

- R1, R2, R3
- R1, R2, R4

To provide protection if node R2 fails, two NNHOP backup tunnels are required: one terminating at R3 and one terminating at R4.
Backup Tunnels Terminating at the Same Destination

The figure below shows how backup tunnels terminating at the same location can be used for redundancy and load balancing. Redundancy and load balancing work for both NHOP and NNHOP backup tunnels.

In this illustration, there are three routers: R1, R2, and R3. At R1, there are two NNHOP backup tunnels (T1 and T2) that go from R1 to R3 without traversing R2.

With redundancy, if R2 fails or the link from R1 to R2 fails, either backup tunnel can be used. If one backup tunnel is down, the other can be used. LSPs are assigned to backup tunnels when the LSPs are first established. This is done before a failure.

With load balancing, if neither backup tunnel has enough bandwidth to back up all LSPs, both tunnels can be used. Some LSPs will use one backup tunnel, other LSPs will use the other backup tunnel. The router decides the best way to fit the LSPs onto the backup tunnels.

Backup Tunnel Selection Procedure

When an LSP is signaled, each node along the LSP path that provides FRR protection for the LSP selects a backup tunnel for the LSP to use if either of the following events occurs:

- The link to the next hop fails.
- The next hop fails.

By having the node select the backup tunnel for an LSP before a failure occurs, the LSP can be rerouted onto the backup tunnel quickly if there is a failure.

For an LSP to be mapped to a backup tunnel, all of the following conditions must exist:

- The LSP is protected by FRR; that is, the LSP is configured with the `tunnel mpls traffic-eng fast-reroute` command.
- The backup tunnel is up.
- The backup tunnel is configured to have an IP address, typically a loopback address.
- The backup tunnel is configured to protect this LSP’s outgoing interface; that is, the interface is configured with the `mpls traffic-eng backup-path` command.
- The backup tunnel does not traverse the LSP’s protected interface.
• The backup tunnel terminates at the LSP's NHOP or NNHOP. If it is an NNHOP tunnel, it does not traverse the LSP's NHOP.

• The bandwidth protection requirements and constraints, if any, for the LSP and backup tunnel are met. For information about bandwidth protection considerations, see the Bandwidth Protection, on page 53.

### Bandwidth Protection

A backup tunnel can be configured to protect two types of backup bandwidth:

- **Limited backup bandwidth**—A backup tunnel provides bandwidth protection. The sum of the bandwidth of all LSPs using this backup tunnel cannot exceed the backup tunnel's backup bandwidth. When assigning LSPs to this type of backup tunnel, sufficient backup bandwidth must exist.

- **Unlimited backup bandwidth**—The backup tunnel does not provide any bandwidth protection (that is, best-effort protection exists). There is no limit to the amount of bandwidth used by the LSPs that are mapped to this backup tunnel. LSPs that allocate zero bandwidth can only use backup tunnels that have unlimited backup bandwidth.

### Load Balancing on Limited-bandwidth Backup Tunnels

There may be more than one backup tunnel that has sufficient backup bandwidth to protect a given LSP. In this case, the router chooses the one that has the least amount of backup bandwidth available. This algorithm limits fragmentation, maintaining the largest amount of backup bandwidth available.

Specifying limited backup bandwidth does not “guarantee” bandwidth protection if there is a link or node failure. For example, the set of NHOP and NNHOP backup tunnels that gets triggered when an interface fails may all share some link on the network topology, and this link may not have sufficient bandwidth to support all LSPs using this set of backup tunnels.

In the figure below, both backup tunnels traverse the same links and hop. When the link between routers R1 and R4 fails, backup tunnels for primary tunnel 1 and primary tunnel 2 are triggered simultaneously. The two backup tunnels may share a link in the network.

**Figure 11: Backup Tunnels Share a Link**

![Backup Tunnels Share a Link](image)
In the figure below, the backup tunnel for primary tunnel 1 may traverse routers R1-R2-R3-R4, and the backup tunnel for primary tunnel 2 may traverse routers R4-R2-R3-R1. In this case, the link R2-R3 may get overloaded if R1-R4 fails.

![Figure 12: Overloaded Link](image)

**Load Balancing on Unlimited-bandwidth Backup Tunnels**

More than one backup tunnel, each having unlimited backup bandwidth, can protect a given interface. In this case, when choosing a backup tunnel for a given LSP, the router chooses the backup tunnel that has the least amount of backup bandwidth in use. This algorithm evenly distributes the LSPs across backup tunnels based on LSP’s bandwidth. If an LSP is requesting zero bandwidth, the router chooses the backup tunnel that is currently protecting the fewest LSPs.

**Pool Type and Backup Tunnels**

By default, a backup tunnel provides protection for LSPs that allocate from any pool (that is, global or subpool). However, a backup tunnel can be configured to protect only LSPs that use global pool bandwidth, or only those that use subpool bandwidth.

**Tunnel Selection Priorities**

This section describes the following:

**NHOP Versus NNHOP Backup Tunnels**

More than one backup tunnel can protect a given LSP, where one backup tunnel terminates at the LSP’s NNHOP, and the other terminates at the LSP’s NHOP. In this case, the router chooses the backup tunnel that terminates at the NNHOP (that is, FRR prefers NNHOP over NHOP backup tunnels).

The table below lists the tunnel selection priorities. The first choice is an NNHOP backup tunnel that acquires its bandwidth from a subpool or global pool, and has limited bandwidth. If there is no such backup tunnel, the next choice (2) is a next-next hop backup tunnel that acquires a limited amount of bandwidth from any pool. The preferences go from 1 (best) to 8 (worst), where choice 3 is for an NNHOP backup tunnel with an unlimited amount of subpool or global pool bandwidth.
Table 4: Tunnel Selection Priorities

<table>
<thead>
<tr>
<th>Preference</th>
<th>Backup Tunnel Destination</th>
<th>Bandwidth Pool</th>
<th>Bandwidth Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (Best)</td>
<td>NNHOP</td>
<td>Subpool or global pool</td>
<td>Limited</td>
</tr>
<tr>
<td>2</td>
<td>NNHOP</td>
<td>Any</td>
<td>Limited</td>
</tr>
<tr>
<td>3</td>
<td>NNHOP</td>
<td>Subpool or global pool</td>
<td>Unlimited</td>
</tr>
<tr>
<td>4</td>
<td>NNHOP</td>
<td>Any</td>
<td>Unlimited</td>
</tr>
<tr>
<td>5</td>
<td>NHOP</td>
<td>Subpool or global pool</td>
<td>Limited</td>
</tr>
<tr>
<td>6</td>
<td>NHOP</td>
<td>Any</td>
<td>Limited</td>
</tr>
<tr>
<td>7</td>
<td>NHOP</td>
<td>Subpool or global pool</td>
<td>Unlimited</td>
</tr>
<tr>
<td>8 (Worst)</td>
<td>NHOP</td>
<td>Any</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

The figure below shows an example of the backup tunnel selection procedure based on the designated amount of global pool and subpool bandwidth currently available.

**Note**

If NHOP and NNHOP backup tunnels do not have sufficient backup bandwidth, no consideration is given to the type of data that the LSP is carrying. For example, a voice LSP may not be protected unless it is signalled before a data LSP. To prioritize backup tunnel usage, see the "Backup Protection Preemption Algorithms" section.

*Figure 13: Choosing from Among Multiple Backup Tunnels*
In this example, an LSP requires 20 units (kilobits per second) of subpool backup bandwidth. The best backup tunnel is selected as follows:

1. Backup tunnels T1 through T4 are considered first because they terminate at the NNHOP.
2. Tunnel T4 is eliminated because it only has 10 units of subpool backup bandwidth.
3. Tunnel T1 is eliminated because it protects only LSPs using global pool bandwidth.
4. Tunnel T3 is chosen over T2 because, although both have sufficient backup bandwidth, T3 has the least backup bandwidth available (leaving the most backup bandwidth available on T2).
5. Tunnels T5 and T6 need not be considered because they terminate at an NHOP, and therefore are less desirable than T3, which terminates at an NNHOP.

**Promotion**

After a backup tunnel has been chosen for an LSP, conditions may change that will cause us to reevaluate this choice. This reevaluation, if successful, is called promotion. Such conditions may include:

1. A new backup tunnel comes up.
2. The currently chosen backup tunnel for this LSP goes down.
3. A backup tunnel’s available backup bandwidth increases. For example, an LSP protected by the tunnel has been reoptimized by the headend to use another path.
4. A backup tunnel’s available backup-bandwidth decreases.

For cases 1 and 2, the LSP’s backup tunnel is evaluated immediately. Cases 3 and 4 are addressed by periodically reevaluating LSP-to-backup tunnel mappings. By default, background reevaluation is performed every 5 minutes. This interval is configurable via the `mpls traffic-eng fast-reroute timers` command.

The response to case 4 is as follows:

When the backup tunnel’s bandwidth is reduced, promotion will not be run so long as the remaining bandwidth is greater than the sum of the bandwidths of all primary paths for which this tunnel is the backup. This policy prevents unnecessary disruption of protection of the primary paths.

When the backup tunnel’s bandwidth does fall below the required bandwidth needed for it to substitute for all primary paths to which it has been assigned, promotion is run.

**Backup Protection Preemption Algorithms**

When you set the “bandwidth protection desired” bit for an LSP, the LSP has a higher right to select backup tunnels that provide bandwidth protection and it can preempt other LSPs that do not have that bit set.

If there is insufficient backup bandwidth on NNHOP backup tunnels but not on NHOP backup tunnels, the bandwidth-protected LSP does not preempt NNHOP LSPs; it uses NHOP protection.

If there are multiple LSPs using a given backup tunnel and one or more must be demoted to provide bandwidth, there are two user-configurable methods (algorithms) that the router can use to determine which LSPs are demoted.

- Minimize amount of bandwidth that is wasted.
- Minimize the number of LSPs that are demoted.
For example, if you need 10 units of backup bandwidth on a backup tunnel, you can demote one of the following:

- A single LSP using 100 units of bandwidth—Makes available more bandwidth than needed, but results in lots of waste
- Ten LSPs, each using one unit of bandwidth—Results in no wasted bandwidth, but affects more LSPs

The default algorithm minimizes the number of LSPs that are demoted. To change the algorithm to minimize the amount of bandwidth that is wasted, enter the `mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw` command.

**Bandwidth Protection Considerations**

There are numerous ways in which bandwidth protection can be ensured. The table below describes the advantages and disadvantages of three methods.

*Table 5: Bandwidth Protection Methods*

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserve bandwidth for backup tunnels explicitly.</td>
<td>It is simple.</td>
<td>It is a challenge to allow bandwidth sharing of backup tunnels protecting against independent failures.</td>
</tr>
<tr>
<td>Use backup tunnels that are signaled with zero bandwidth.</td>
<td>It provides a way to share bandwidth used for protection against independent failures, so it ensures more economical bandwidth usage.</td>
<td>It may be complicated to determine the proper placement of zero bandwidth tunnels.</td>
</tr>
<tr>
<td>Backup bandwidth protection</td>
<td>Ensures bandwidth protection for voice traffic.</td>
<td>An LSP that does not have backup bandwidth protection can be demoted at any time if there is not enough backup bandwidth and an LSP that has backup bandwidth protection needs bandwidth.</td>
</tr>
</tbody>
</table>

Cisco implementation of FRR does not mandate a particular approach, and it provides the flexibility to use any of the above approaches. However, given a range of configuration choices, be sure that the choices are constant with a particular bandwidth protection strategy.

The following sections describe some important issues in choosing an appropriate configuration:

**Using Backup Tunnels with Explicitly Signaled Bandwidth**

There are two bandwidth parameters that must be set for a backup tunnel:

- actual signaled bandwidth
- backup-bandwidth
To signal bandwidth requirements of a backup tunnel, configure the bandwidth of the backup tunnel by using the `tunnel mpls traffic-eng bandwidth` command.

To configure the backup bandwidth of the backup tunnel, use the `tunnel mpls traffic-eng backup-bw` command.

The signaled bandwidth is used by the LSRs on the path of the backup tunnel to perform admission control and do appropriate bandwidth accounting.

The backup bandwidth is used by the PLR (the headend of the backup tunnel) to decide how much primary traffic can be rerouted to this backup tunnel if there is a failure.

Both parameters need to be set to ensure proper operation. The numerical value of the signaled bandwidth and the backup-bandwidth should be the same.

**Protected Bandwidth Pools and the Bandwidth Pool from Which the Backup Tunnel Reserves Its Bandwidth**

The `tunnel mpls traffic-eng bandwidth` command allows you to configure the following:

- Amount of bandwidth a backup tunnel reserves
- The DS-TE bandwidth pool from which the bandwidth needs to be reserved

**Note**

Only one pool can be selected (that is, the backup tunnel can explicitly reserve bandwidth from either the global pool or the subpool, but not both).

The `tunnel mpls traffic-eng backup-bw` command allows you to specify the bandwidth pool to which the traffic must belong for the traffic to use this backup tunnel. Multiple pools are allowed.

There is no direct correspondence between the bandwidth pool that is protected and the bandwidth pool from which the bandwidth of the backup tunnel draws its bandwidth.

Example: In this example, assume the following:

- Bandwidth protection is desired only for subpool traffic, but the best-effort traffic using the global pool does not require bandwidth protection.
- Scheduling is configured so that subpool traffic uses the priority queue, and global pool traffic is served at a lower priority.

Bandwidth protection for 10 Kbps of subpool traffic on a given link can be achieved by any of the following combinations:

- `tunnel mpls traffic-eng bandwidth sub-pool 10`
- `tunnel mpls traffic-eng backup-bw sub-pool 10`
- `tunnel mpls traffic-eng bandwidth global-pool 10`
- `tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool unlimited`
- `tunnel mpls traffic-eng bandwidth global-pool 40`
- `tunnel mpls traffic-eng backup-bw sub-pool 10 global-pool 30`
Using Backup Tunnels Signaled with Zero Bandwidth

Frequently it is desirable to use backup tunnels with zero signaled bandwidth, even when bandwidth protection is required. It may seem that if no bandwidth is explicitly reserved, no bandwidth guarantees can be provided. However, that is not necessarily true.

In the following situation:

- Only link protection is desired.
- Bandwidth protection is desired only for subpool traffic.

For each protected link AB with a max reservable subpool value of S, there may be a path from node A to node B such that the difference between max reservable global and max reservable subpool is at least S. If it is possible to find such paths for each link in the network, you can establish all the backup tunnels along such paths without any bandwidth reservations. If there is a single link failure, only one backup tunnel will use any link on its path. Because that path has at least S of available bandwidth (in the global pool), assuming that marking and scheduling is configured to classify the subpool traffic into a priority queue, the subpool bandwidth is guaranteed.

The above approach allows sharing of the global pool bandwidth between backup tunnels protecting independent link failures. The backup tunnels are expected to be used for only a short period of time after a failure (until the headends of affected LSPs reroute those LSPs to other paths with available subpool bandwidth). The probability of multiple unrelated link failures is very small (in the absence of node or SRLG failures, which result in multiple link failures). Therefore, it is reasonable to assume that link failures are in practice independent with high probability. This "independent failure assumption" in combination with backup tunnels signaled without explicit bandwidth reservation enables efficient bandwidth sharing that yields substantial bandwidth savings.

Backup tunnels protecting the subpool traffic do now draw bandwidth from any pool. Primary traffic using the global pool can use the entire global pool, and primary traffic using the subpool can use the entire subpool. Yet, subpool traffic has a complete bandwidth guarantee if there is a single link failure.

A similar approach can be used for node and SRLG protection. However, the decision of where to put the backup tunnels is more complicated because both node and SRLG failures effectively result in the simultaneous failure of several links. Therefore, the backup tunnels protecting traffic traversing all affected links cannot be computed independently of each other. The backup tunnels protecting groups of links corresponding to different failures can still be computed independently of each other, which results in similar bandwidth savings.

Signaled Bandwidth Versus Backup Bandwidth

Backup bandwidth is used locally (by the router that is the headend of the backup tunnel) to determine which, and how many, primary LSPs can be rerouted on a particular backup tunnel. The router ensures that the combined bandwidth requirement of these LSPs does not exceed the backup bandwidth.

Therefore, even when the backup tunnel is signaled with zero bandwidth, the backup bandwidth must be configured with the value corresponding to the actual bandwidth requirement of the traffic protected by this backup tunnel. Unlike the case when bandwidth requirements of the backup tunnels are explicitly signaled, the value of the signaled bandwidth (which is zero) is not the same value as the backup bandwidth.
### How to Configure MPLS TE Link and Node Protection with RSVP Hellos Support

This section assumes that you want to add FRR protection to a network in which MPLS TE LSPs are configured. Make sure that the following tasks have been performed before you perform the configuration tasks, but you do not have to already have configured MPLS TE tunnels:

- Enabled MPLS TE on all relevant routers and interfaces
- Configured MPLS TE tunnels

The following sections describe how to use FRR to protect LSPs in your network from link or node failures. Each task is identified as either required or optional.

#### Note
You can perform the configuration tasks in any order.

#### Note
An NNHOP backup tunnel must not go via the NHOP.

### Enabling Fast Reroute on LSPs

LSPs can use backup tunnels only if they have been configured as fast reroutable. To do this, enter the following commands at the headend of each LSP.

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `tunnel mpls traffic-eng fast-reroute [bw-protect]`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| Router> enable | |

---

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `tunnel mpls traffic-eng fast-reroute [bw-protect]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Example:

| Router> enable | |

---
<table>
<thead>
<tr>
<th>Step 2</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface tunnel number</td>
<td>Enters interface configuration mode for the specified tunnel.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface tunnel 1000</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>tunnel mpls traffic-eng fast-reroute [bw-protect]</td>
<td>Enables an MPLS TE tunnel to use an established backup tunnel if there is a link or node failure.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect</td>
<td></td>
</tr>
</tbody>
</table>

**Creating a Backup Tunnel to the Next Hop or to the Next-Next Hop**

To create a backup tunnel to the next hop or to the next-next hop, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the “Feature Information for MPLS TE Link and Node Protection with RSVP Hellos Support,” for more information.

Creating a backup tunnel is basically no different from creating any other tunnel. None of the commands below is new.

**Note**

When using the `exclude-address` command to specify the path for a backup tunnel, you must exclude an interface address to avoid a link (for creating an NHOP backup tunnel), or a router-ID address to avoid a node (for creating an NNHOP backup tunnel).
SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. ip unnumbered type number
5. tunnel destination A.B.C.D
6. tunnel mode mpls traffic-eng
7. tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name | path-number}} [lockdown]
8. ip explicit-path name name
9. exclude-address address

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 interface tunnel number</td>
<td>Creates a new tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface tunnel 1</td>
<td></td>
</tr>
<tr>
<td>Step 4 ip unnumbered type number</td>
<td>Gives the tunnel interface an IP address that is the same as that of interface Loopback0.</td>
</tr>
<tr>
<td>Example:</td>
<td>Note: This command is not effective until Lookback0 has been configured with an IP address.</td>
</tr>
<tr>
<td>Router(config-if)# ip unnumbered loopback0</td>
<td></td>
</tr>
<tr>
<td>Step 5 tunnel destination A.B.C.D</td>
<td>Specifies the IP address of the device where the tunnel will terminate.</td>
</tr>
<tr>
<td>Example:</td>
<td>• That address should be the router ID of the device that is the NHOP or NNHOP of LSPs to be protected.</td>
</tr>
<tr>
<td>Router(config-if)# tunnel destination 10.3.3.3</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 6</strong> tunnel mode mpls traffic-eng</td>
<td>Sets encapsulation mode of the tunnel to MPLS TE.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# tunnel mode mpls traffic-eng</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> tunnel mpls traffic-eng path-option number</td>
<td>Configures a path option for an MPLS TE tunnel.</td>
</tr>
<tr>
<td>{dynamic}</td>
<td>explicit {name path-name}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# tunnel mpls traffic-eng path-option 300 explicit name avoid-protected-link</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> ip explicit-path name name</td>
<td>Enters the subcommand mode for IP explicit paths to create the named path.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip explicit-path name avoid-protected-link</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> exclude-address address</td>
<td>For Link Protection, specifies the IP address of the link to be protected.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>• For Node Protection, this command specifies the router ID of the node to be protected.</td>
</tr>
<tr>
<td>Router(cfg-ip-expl-path)# exclude-address 10.3.3.3</td>
<td>Note</td>
</tr>
<tr>
<td>Backup tunnel paths can be dynamic or explicit and they do not have to use exclude-address. Because backup tunnels must avoid the protected link or node, it is convenient to use an exclude-address.</td>
<td></td>
</tr>
</tbody>
</table>

## Assigning Backup Tunnels to a Protected Interface

To assign one or more backup tunnels to a protected interface, enter the following commands on the node that will be the headend of the backup tunnel (that is, the node whose downstream link or node may fail). The node on which you enter these commands must be a supported platform. See the Finding Feature Information section.

### Note
You must configure the interface to have an IP address and to enable the MPLS TE tunnel feature.
### SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port
4. mpls traffic-eng backup-path tunnel interface

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface type slot / port</td>
<td>Moves configuration to the physical interface level, directing</td>
</tr>
<tr>
<td>Example:</td>
<td>subsequent configuration commands to the specific physical interface</td>
</tr>
<tr>
<td>Example:</td>
<td>identified by the type value.</td>
</tr>
<tr>
<td>Example:</td>
<td>The slot and port identify the slot and port being configured.</td>
</tr>
<tr>
<td>Example:</td>
<td>The interface must be a supported interface. See the Finding Feature</td>
</tr>
<tr>
<td>Example:</td>
<td>Information section. Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface POS 5/0</td>
</tr>
<tr>
<td><strong>Step 4</strong> mpls traffic-eng backup-path tunnel</td>
<td>Allows LSPs going out this interface to use this backup tunnel if there</td>
</tr>
<tr>
<td>interface</td>
<td>is a link or node failure.</td>
</tr>
<tr>
<td>Example:</td>
<td><strong>Note</strong> You can enter this command multiple times to associate</td>
</tr>
<tr>
<td>Example:</td>
<td>multiple backup tunnels with the same protected interface.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# mpls traffic-eng backup-path tunnel 2</td>
</tr>
</tbody>
</table>
Associating Backup Bandwidth and Pool Type with a Backup Tunnel

To associate backup bandwidth with a backup tunnel and designate the type of LSP that can use a backup tunnel, enter the following commands.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `tunnel mpls traffic-eng backup-bw {bandwidth | [sub-pool {bandwidth | Unlimited}] [global-pool {bandwidth | Unlimited}]}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `enable` | Enables privileged EXEC mode.  
  *Enter your password if prompted.* |
| Example: | `Router> enable` |
| Step 2 | `configure terminal` | Enters global configuration mode. |
| Example: | `Router# configure terminal` |
| Step 3 | `interface tunnel number` | Enters interface configuration mode for the specified tunnel. |
| Example: | `Router(config)# interface tunnel 2` |
| Step 4 | `tunnel mpls traffic-eng backup-bw {bandwidth | [sub-pool {bandwidth | Unlimited}] [global-pool {bandwidth | Unlimited}]}` | Associates bandwidth with a backup tunnel and designates whether LSPs that allocate bandwidth from the specified pool can use the tunnel. |
| Example: | `Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000` |
Configuring Backup Bandwidth Protection

SUMMARY STEPS

1. enable
2. configure terminal
3. tunnel mpls traffic-eng fast-reroute [bw-protect]
4. mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: <code>Router&gt; enable</code></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: <code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> tunnel mpls traffic-eng fast-reroute [bw-protect]</td>
<td>Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.</td>
</tr>
<tr>
<td>Example: <code>Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect</code></td>
<td>• The <strong>bw-protect</strong> keyword gives an LSP priority for using backup tunnels with bandwidth protection. Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong> mpls traffic-eng fast-reroute backup-prot-preemption [optimize-bw]</td>
<td>Changes the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.</td>
</tr>
<tr>
<td>Example: <code>Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw</code></td>
<td></td>
</tr>
</tbody>
</table>

Configuring an Interface for Fast Link and Node Failure Detection

To configure an interface for fast link and node failure detection, perform the following steps.
SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot / port
4. pos ais-shut
5. pos report \{b1-tca | b2-tca | b3-tca | lais | lrdi | pais | plop | prdi | rdool | sd-ber | sf-ber | slof | slos\}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>      • Enter your password if prompted.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>interface type slot / port</td>
</tr>
<tr>
<td>Example: Router(config)# interface pos0/0</td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>pos ais-shut</td>
</tr>
<tr>
<td>Example: Router(config-if)# pos ais-shut</td>
<td>Sends the line alarm indication signal (LAIS) when the Packet-over-SONET (POS) interface is placed in any administrative shutdown state.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>pos report {b1-tca</td>
</tr>
<tr>
<td>Example: Router(config-if)# pos report lrdi</td>
<td>Permits selected SONET alarms to be logged to the console for a POS interface.</td>
</tr>
</tbody>
</table>

Configuring an Interface for Fast Tunnel Interface Down

To configure an interface for fast tunnel interface down, perform the following steps.
# SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface type slot / port`
4. `tunnel mpls traffic-eng interface down delay time`

# DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface <code>type slot / port</code></td>
<td>Configures an interface type and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config)# interface tunnel 1000</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> <code>tunnel mpls traffic-eng interface down delay time</code></td>
<td>Forces a tunnel to go down as soon as the headend router detects that the LSP is down.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# tunnel mpls traffic-eng interface down delay 0</code></td>
<td></td>
</tr>
</tbody>
</table>

## Verifying That Fast Reroute Is Operational

To verify that FRR can function, perform the following steps.
SUMMARY STEPS

1. show mpls traffic-eng tunnels brief
2. show ip rsvp sender detail
3. show mpls traffic-eng fast-reroute database
4. show mpls traffic-eng tunnels backup
5. show mpls traffic-eng fast-reroute database
6. show ip rsvp reservation

DETAILED STEPS

Step 1  show mpls traffic-eng tunnels brief
Use this command to verify that backup tunnels are up:

Example:

Router# show mpls traffic-eng tunnels brief

Signalling Summary:
LSP Tunnels Process: running
RSVP Process: running
Forwarding: enabled
Periodic reoptimization: every 3600 seconds, next in 1706 seconds
TUNNEL NAME DESTINATION UP IF DOWN IF STATE/PROT
Router_t1 10.112.0.12 - PO4/0/1 up/up
Router_t2 10.112.0.12 - unknown up/down
Router_t3 10.112.0.12 - unknown admin-down
Router_t1000 10.110.0.10 - unknown up/down
Router_t2000 10.110.0.10 - PO4/0/1 up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails

Step 2  show ip rsvp sender detail
Use this command to verify that LSPs are protected by the appropriate backup tunnels.

Following is sample output from the show ip rsvp sender detail command when the command is entered at the PLR before a failure:

Example:

Router# show ip rsvp sender detail

PATH:
Tun Dest: 10.10.0.6 Tun ID: 100 Ext Tun ID: 10.10.0.1
Tun Sender: 10.10.0.1 LSP ID: 31
Path refreshes: arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
Session Attr:
Setup Prio: 7, Holding Prio: 7
Flags: (0x7) Local Prot desired, Label Recording, SE Style
session Name: R1_t100
ERO: (incoming)
10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
RRO:
10.10.7.1/32, Flags:0x0 (No Local Protection)
10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP) !Available to NNHOP
10.10.1.1/32, Flags:0x0 (No Local Protection)
Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: No backup tunnel selected
  Path ID handle: 50000416.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxy-terminated

Step 3

show mpls traffic-eng fast-reroute database
Enter the clear ip rsvp hello instance counters command to verify the following:

- MPLS TE FRR Node Protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

Example:

Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected tunnel    In-label Out intf/label FRR intf/label Status
Tunnel500          Tun hd AT4/0.100:Untagg Tu501:20 ready
Prefix item frr information:
Prefix    Tunnel In-label Out intf/label FRR intf/label Status
10.0.0.8/32  Tu500 18 AT4/0.100:Pop ta Tu501:20 ready
10.0.8.9/32  Tu500 19 AT4/0.100:Untagg Tu501:20 ready
10.8.9.0/24  Tu500 22 AT4/0.100:Untagg Tu501:20 ready
LSP midpoint item frr information:
LSP identifier In-label Out intf/label FRR intf/label Status
If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the show mpls forwarding-table ip-address detail command. The final line of the display will tell whether that prefix is protected:

Example:

Router# show mpls forwarding-table 10.0.0.11 32 detail
Local Outgoing Prefix Bytes tag Outgoing Next Hop
tag tag or VC or Tunnel Id switched interface
Tun hd Untagged 10.0.0.11/32 48 pos5/0 point2point
MAC/Encaps=4/8, MTU=1520, Tag Stack(22)
48D18847 00016000
No output feature configured
Fast Reroute Protection via (Tu0, outgoing label 12304)
The following command output displays the LSPs that are protected when the FRR primary tunnel is over an ATM interface and the backup tunnel is over a POS interface. As shown in the figure below, interface ATM4/0.100 is protected by backup tunnel 501.

**Figure 14: Protected LSPs**

![Diagram showing protected LSPs](image)

This figure displays the protected LSPs:

- The primary tunnel is 500 and the path is R1 via ATM4/0.100 to R2, from R2 to R3, and from R3 to R4.
- The FRR backup tunnel is 501 and the path is R1 via POS2/0 to R2.
- The interface ATM4/0.100 is protected by the backup tunnel 501.

**Example:**

Router# `show mpls traffic-eng fast-reroute database`

**Tunnel head end item frr information:**

<table>
<thead>
<tr>
<th>Protected tunnel</th>
<th>In-label</th>
<th>Out intf/label</th>
<th>FRR intf/label</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel500</td>
<td>Tun hd</td>
<td>AT4/0.100:Untagg</td>
<td>Tu501:20</td>
<td>ready</td>
</tr>
</tbody>
</table>

**Prefix item frr information:**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Tunnel</th>
<th>In-label</th>
<th>Out intf/label</th>
<th>FRR intf/label</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.8/32</td>
<td>Tu500</td>
<td>18</td>
<td>AT4/0.100:Pop ta Tu501:20</td>
<td>ready</td>
<td></td>
</tr>
<tr>
<td>10.0.8.9/24</td>
<td>Tu500</td>
<td>22</td>
<td>AT4/0.100:Untagg Tu501:20</td>
<td>ready</td>
<td></td>
</tr>
</tbody>
</table>

**LSP midpoint item frr information:**

The following command output displays the LSPs that are protected when the FRR backup tunnel is over an ATM interface:

**Example:**

Router# `show mpls traffic-eng fast-reroute database`

**Tunnel head end item frr information:**

<table>
<thead>
<tr>
<th>Protected tunnel</th>
<th>In-label</th>
<th>Out intf/label</th>
<th>FRR intf/label</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel500</td>
<td>Tun hd</td>
<td>PO2/0:Untagged</td>
<td>Tu501:20</td>
<td>ready</td>
</tr>
</tbody>
</table>

**Prefix item frr information:**

<table>
<thead>
<tr>
<th>Prefix</th>
<th>Tunnel</th>
<th>In-label</th>
<th>Out intf/label</th>
<th>FRR intf/label</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.8/32</td>
<td>Tu500</td>
<td>18</td>
<td>PO2/0:Pop tag Tu501:20</td>
<td>ready</td>
<td></td>
</tr>
<tr>
<td>10.0.8.9/24</td>
<td>Tu500</td>
<td>22</td>
<td>PO2/0:Untagged Tu501:20</td>
<td>ready</td>
<td></td>
</tr>
</tbody>
</table>

**LSP midpoint item frr information:**

**Step 4** `show mpls traffic-eng tunnels backup`
The following conditions must exist for backup tunnels to be operational:

- **LSP is reroutable** -- At the headend of the LSP, enter the `show run int tunnel tunnel-number` command. The output should include the `tunnel mpls traffic-eng fast-reroute` command. If it does not, enter this command for the tunnel.

On the router where the backup tunnels originate, enter the `show mpls traffic-eng tunnels backup` command. Following is sample command output:

```
Example:

Router# show mpls traffic-eng tunnels backup
Router_t578
 LSP Head, Tunnel578, Admin: up, Oper: up
 Src 10.55.55.55, Dest 10.88.88.88, Instance 1
 Fast Reroute Backup Provided:
   Protected i/fs: PO1/0, PO1/1, PO3/3
   Backup BW: any pool unlimited; inuse: 100 kbps

Router_t5710
 LSP Head, Tunnel5710, Admin: admin-down, Oper: down
 Src 10.55.55.55, Dest 10.7.7.7, Instance 0
 Fast Reroute Backup Provided:
   Protected i/fs: PO1/1
   Backup BW: any pool unlimited; inuse: 0 kbps

Router_t5711
 LSP Head, Tunnel5711, Admin: up, Oper: up
 Src 10.55.55.55, Dest 10.7.7.7, Instance 1
 Fast Reroute Backup Provided:
   Protected i/fs: PO1/0
   Backup BW: any pool unlimited; inuse: 6010 kbps
```

The command output will allow you to verify the following:

- **Backup tunnel exists**-- Verify that there is a backup tunnel that terminates at this LSP’s NHOP or NNHOP. Look for the LSP’s NHOP or NNHOP in the Dest field.
- **Backup tunnel is up**-- To verify that the backup tunnel is up, look for “Up” in the State field.
- **Backup tunnel is associated with LSP’s I/F**-- Verify that the interface for the LSP is allowed to use this backup tunnel. Look for the LSP’s output interface in the “protects” field list.
- **Backup tunnel has sufficient bandwidth**-- If you restricted the amount of bandwidth a backup tunnel can hold, verify that the backup tunnel has sufficient bandwidth to hold the LSPs that would use this backup tunnel if there is a failure. The bandwidth of an LSP is defined by the line `tunnel mpls traffic-eng bandwidth` at the headend of the LSP. To determine the available bandwidth on a backup tunnel, look at the “cfg” and “inuse” fields. If there is insufficient backup bandwidth to accommodate the LSPs that would use this backup tunnel in the event of a failure, create an additional backup tunnel or increase the backup bandwidth of the existing tunnel by using the `tunnel mpls traffic-eng bandwidth` command.

**Note** To determine how much bandwidth is sufficient, offline capacity planning may be required.

- **Backup tunnel has appropriate bandwidth type**-- If you restricted the type of LSPs (subpool or global pool) that can use this backup tunnel, verify that the LSP is the appropriate type for the backup tunnel. The type of the LSP is defined by the line `tunnel mpls traffic-eng bandwidth` at the headend of this LSP. If this line contains the word “subpool”, then it uses subpool bandwidth; otherwise, it uses global pool bandwidth. Verify that the type matches the type the backup tunnel can hold by looking in the output of the above command.
If none of the above actions works, enable debug by entering the **debug ip rsvp fast-reroute** command and the **debug mpls traffic-eng fast-reroute** command on the router that is the headend of the backup tunnel. Then do the following:

1. Enter the **shutdown** command for the primary tunnel.
2. Enter the **no shutdown** command for the primary tunnel.
3. View the debug output.

### Step 5

**show mpls traffic-eng fast-reroute database**

Enter the **clear ip rsvp hello instance counters** command to verify the following:

- MPLS TE FRR Node Protection has been enabled.
- A certain type of LSP can use a backup tunnel.

The following command output displays the LSPs that are protected:

**Example:**

```
Router# show mpls traffic-eng fast-reroute database
Tunnel head end item frr information:
Protected Tunnel  In-label intf/label  FRR intf/label  Status
Tunne110  Tun  pos5/0:Untagged  Tu0:12304  ready
Prefix item frr information:
Prefix  Tunnel  In-label  Out intf/label  FRR intf/label  Status
10.0.0.11/32  Tu110  Tun hd  pos5/0:Untagged  Tu0:12304  ready
LSP midpoint frr information:
LSP identifier  In-label  Out intf/label  FRR intf/label  Status
10.0.0.12 1 [459] 16  pos0/1:17  Tu2000:19  ready
```

**Note** If LDP is not enabled, separate prefix items are not shown because all prefixes then use a single rewrite. To confirm that a particular IP prefix is FRR protected, even though it is not shown in this display, enter it within the **show mpls forwarding-table ip-address detail** command. The final line of the display will tell whether that prefix is protected:

**Example:**

```
Router# show mpls forwarding-table 10.0.0.11 32 detail
Local Outgoing Prefix  Bytes tag  Outgoing  Next Hop
tag  tag or VC  or Tunnel Id  switched  interface
Tun hd  Untagged 10.0.0.11/32 48  pos5/0  point2point
MAC/Encaps=4/8, MTU=1520, Tag Stack(22)
48D18847 00016000
No output feature configured
Fast Reroute Protection via (Tu0, outgoing label 12304)
```

### Step 6

**show ip rsvp reservation**

Following is sample output from the **show ip rsvp reservation** command entered at the headend of a primary LSP. Entering the command at the head-end of the primary LSP shows, among other things, the status of FRR (that is, local protection) at each hop this LSP traverses. The per-hop information is collected in the Record Route Object (RRO) that travels with the Resv message from the tail to the head.

**Example:**

```
Router# show ip rsvp reservation detail
Reservation:
```
Notice the following about the primary LSP:

- It has protection that uses a NHOP backup tunnel at its first hop.
- It has protection and is actively using an NHOP backup tunnel at its second hop.
- It has no local protection at its third hop.

The RRO display shows the following information for each hop:

- Whether local protection is available (that is, whether the LSP has selected a backup tunnel)
- Whether local protection is in use (that is, whether the LSP is currently using its selected backup tunnel)
- Whether the selected backup tunnel is an NHOP or NNHOP backup tunnel
- Whether the backup tunnel used at this hop provides bandwidth protection

Troubleshooting Tips

This section describes the following:

LSPs Do Not Become Active; They Remain Ready

At a PLR, LSPs transition from Ready to Active if one of the following events occurs:

- Primary interface goes down--If the primary interface (LSP’s outbound interface) goes down and the LSP is ready to use a backup tunnel, the LSP will transition to the active state causing its data to flow over the backup tunnel. On some platforms and interface types (for example, GSR POS interfaces), fast interface-down logic has been added to detect this event very quickly. On other platforms where this logic does not exist, detection time is slower. On such platforms, it may be desirable to enable RSVP Hello (see the next bulleted item, “Hellos detect next hop is down”).

- Hellos detect next hop is down--If Hellos are enabled on the primary interface (LSP’s outbound interface), and the LSP’s next hop is no longer reachable, the next hop is declared down. This event will cause the LSP to begin actively using its backup tunnel. Notice that a next hop will be declared down even if the primary interface does not go down. For example, if the next hop stops responding due to a reboot or software/hardware problem, Hellos will trigger the LSPs using this next hop to switch to their backup
tunnels. Hellos can also help trigger FRR on interfaces such as Gigabit Ethernet where the interface remains up but is unusable (due to lack of link-layer liveness detection mechanisms).

**Primary Tunnel Does Not Select Backup Tunnel That Is Up**

If a backup tunnel is up, but it is not selected as a backup tunnel by the primary tunnel (LSP), enter the following commands for the backup tunnel:

- `shutdown`
- `no shutdown`

If you change the status of a backup tunnel, the backup tunnel selection algorithm is rerun for the backup tunnel. LSPs that have currently selected (that is, are ready to use) that backup tunnel will be disassociated from it, and then reassocia ted with that backup tunnel or another backup tunnel. This is generally harmless and usually results in mapping the same LSPs to that backup tunnel. However, if any LSPs are actively using that backup tunnel, shutting down the backup tunnel will tear down those LSPs.

---

**Enhanced RSVP Commands**

The following RSVP commands have been enhanced to display information that can be helpful when examining FRR state or when troubleshooting FRR:

- `show ip rsvp request` -- Displays upstream reservation state (that is, information related to the Resv messages that this node will send upstream).
- `show ip rsvp reservation` -- Displays information about Resv messages received.
- `show ip rsvp sender` -- Displays information about Path messages being received.

These commands show control plane state; they do not show data state. That is, they show information about RSVP messages (Path and Resv) used to signal LSPs. For information about the data packets being forwarded along LSPs, use the `show mpls forwarding` command.

**RSVP Hello**

The RSVP Hello feature enables RSVP nodes to detect when a neighboring node is not reachable. Use this feature when notification of link-layer failures is not available and unnumbered links are not used, or when the failure detection mechanisms provided by the link layer are not sufficient for timely node failure detection. Hello must be configured both globally on the router and on the specific interface to be operational.

**Hello Instances Have Not Been Created**

If Hello instances have not been created, do the following:

- Determine if RSVP Hello has been enabled globally on the router. Enter the `ip rsvp signalling hello` (configuration) command.
- Determine if RSVP Hello has been enabled on an interface that the LSPs traverse. Enter the `ip rsvp signalling hello` (interface) command.
- Verify that at least one LSP has a backup tunnel by viewing the output of the `show ip rsvp sender` command. A value of "Ready" indicates that a backup tunnel has been selected.
No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)"

Error Message Is Printed at the Point of Local Repair

FRR relies on a Record Route Object (RRO) in Resv messages arriving from downstream. Routers receiving Path messages with the SESSION_ATTRIBUTE bit indicating that the LSP is fast-reroutable should include an RRO in the corresponding Resv messages.

If an LSP is configured for FRR, but the Resv arriving from a downstream router contains an incomplete RRO, the "No entry at index (error may self-correct, RRO may not yet have propagated from downstream node of interest)" message is printed. An incomplete RRO is one in which the NHOP or the NNHOP did not include an entry in the RRO.

This error typically means that backup tunnels to the NHOP or the NNHOP cannot be selected for this LSP because there is insufficient information about the NHOP or NNHOP due to the lack of an RRO entry.

Occasionally there are valid circumstances in which this situation occurs temporarily and the problem is self-corrected. If subsequent Resv messages arrive with a complete RRO, ignore the error message.

To determine whether the error has been corrected, view the RRO in Resv messages by entering the `clear ip rsvp hello instance counters` command. Use an output filter keyword to view only the LSP of interest.

Couldn’t get rsbs (error may self-correct when Resv arrives)"

Error Message Is Printed at the Point of Local Repair

The PLR cannot select a backup tunnel for an LSP until a Resv message has arrived from downstream.

When this error occurs, it typically means that something is truly wrong. For example, no reservation exists for this LSP. You can troubleshoot this problem by using the `debug ip rsvp reservation` command to enable debug.

Occasionally there are valid circumstances in which this error message occurs and there is no need for concern. One such circumstance is when an LSP experiences a change before any Resv message has arrived from downstream. Changes can cause a PLR to try to select a backup tunnel for an LSP, and the selection will fail (causing this error message) if no Resv message has arrived for this LSP.
Config Examples for MPLS TE Link and Node Protection with RSVP Hellos Support

The examples relate to the illustration shown below.

Figure 15: Backup Tunnels

---

**Enabling Fast Reroute for All Tunnels Example**

On router R1, enter interface configuration mode for each tunnel to be protected (Tunnel 1000 and Tunnel 2000). Enable these tunnels to use a backup tunnel in case of a link or node failure along their paths.

Tunnel 1000 will use 10 units of bandwidth from the subpool.

Tunnel 2000 will use 5 units of bandwidth from the global pool. The “bandwidth protection desired” bit and the “node protection desired bit” have been set by specifying `bw-prot` and `node-prot`, respectively, in the `tunnel mpls traffic-eng fast-reroute` command.

```
Router(config)# interface Tunnel1000
Router(config-if)# tunnel mpls traffic-eng fast-reroute
Router(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 10
Router(config)# interface Tunnel2000
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-prot node-prot
Router(config-if)# tunnel mpls traffic-eng bandwidth 5
```
Creating an NHOP Backup Tunnel Example

On router R2, create an NHOP backup tunnel to R3. This backup tunnel should avoid using the link 10.1.1.2.

```
Router(config)# ip explicit-path name avoid-protected-link
Router(cfg-ip-expl-path)# exclude-address 10.1.1.2

Explicit Path name avoid-protected-link:
___1: exclude-address 10.1.1.2
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel1
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.3.3.3
Router(config-if)# tunnel mode mpls traffic-eng0
Router(config-if)# tunnel mpls traffic-eng path-option explicit avoid-protected-link
```

Creating an NNHOP Backup Tunnel Example

On router R2, create an NNHOP backup tunnel to R4. This backup tunnel should avoid R3.

```
Router(config)# ip explicit-path name avoid-protected-node
Router(cfg-ip-expl-path)# exclude-address 10.3.3.3

Explicit Path name avoid-protected-node:
___1: exclude-address 10.3.3.3
Router(cfg-ip_expl-path)# end

Router(config)# interface Tunnel2
Router(config-if)# ip unnumbered loopback0
Router(config-if)# tunnel destination 10.4.4.4
Router(config-if)# tunnel mode mpls traffic-eng0
Router(config-if)# tunnel mpls traffic-eng path-option explicit avoid-protected-node
```

Assigning Backup Tunnels to a Protected Interface Example

On router R2, associate both backup tunnels with interface POS5/0.

```
Router(config)# interface POS5/0
Router(config-if)# mpls traffic-eng backup-path tunnel1
Router(config-if)# mpls traffic-eng backup-path tunnel2
Associating Backup Bandwidth and Pool Type with Backup Tunnels Example

Backup tunnel 1 is to be used only by LSPs that take their bandwidth from the global pool. It does not provide bandwidth protection. Backup tunnel 2 is to be used only by LSPs that take their bandwidth from the subpool. Backup tunnel 2 provides bandwidth protection for up to 1000 units.

Router(config)# interface Tunnel1
Router(config-if)# tunnel mpls traffic-eng backup-bw global-pool Unlimited
Router(config)# interface Tunnel2
Router(config-if)# tunnel mpls traffic-eng backup-bw sub-pool 1000

Configuring Backup Bandwidth Protection Example

In the following example, backup bandwidth protection is configured.

This global configuration is required only to change the backup protection preemption algorithm from minimize the number of LSPs that are demoted to minimize the amount of bandwidth that is wasted.

Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
Router(config)# mpls traffic-eng fast-reroute backup-prot-preemption optimize-bw

Configuring an Interface for Fast Link and Node Failure Detection Example

In the following example, pos ais-shut is configured:

Router(config)# interface pos0/0/0
Router(config-if)# pos ais-shut

In the following example, report lrdi is configured on OS interfaces:

Router(config)# interface pos0/0/0
Router(config-if)# pos report lrdi

Configuring an Interface for Fast Tunnel Interface Down Example

In the following example, tunnel 1000 goes down as soon as the headend router detects that the LSP is down:

Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng interface down delay 0
**Configuring RSVP Hello and POS Signals Example**

Hello must be configured both globally on the router and on the specific interface on which you need FRR protection. To configure Hello, use the following configuration commands:

- `ip rsvp signalling hello` (configuration)--Enables Hello globally on the router.
- `ip rsvp signalling hello` (interface)--Enables Hello on an interface where you need FRR protection.

The following configuration commands are optional:

- `ip rsvp signalling hello dscp` --Sets the DSCP value that is in the IP header of the Hello message.
- `ip rsvp signalling hello refresh misses` --Specifies how many acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down.
- `ip rsvp signalling hello refresh interval` --Configures the Hello request interval.
- `ip rsvp signalling hello statistics` --Enables Hello statistics on the router.

For configuration examples, see the Hello command descriptions in the "Command Reference" section of MPLS Traffic Engineering (TE): Link and Node Protection, with RSVP Hellos Support.

To configure POS signaling for detecting FRR failures, enter `pos report all` or enter the following commands to request individual reports:

```plaintext
pos ais-shut
pos report rdool
pos report lais
pos report lrdi
pos report pais
pos report prdi
pos report sd-ber
```

**Additional References**

The following sections provide references related to the MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) feature.

**Related Documents**

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-IS</td>
<td>• Cisco IOS IP Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>• Configuring a Basic IS-IS Network</td>
</tr>
<tr>
<td>MPLS traffic engineering commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OSPF</td>
<td>• Cisco IOS IP Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>• Configuring OSPF</td>
</tr>
<tr>
<td>RSVP commands</td>
<td>• Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
</tbody>
</table>

**Standards**

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>
Technical Assistance

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

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.

- `tunnel mpls traffic-eng interface down delay`

Feature Information for MPLS TE Link and Node Protection with RSVP Hellos 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.
### Feature Information for MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</td>
<td>12.0(10)ST</td>
<td>The MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) feature provides the following Fast Reroute (FRR) capabilities:</td>
</tr>
<tr>
<td></td>
<td>12.0(16)ST</td>
<td>• A backup tunnel terminates at the next-next hop router to protect both the downstream link and node in order to protect link and node failures. There is no limit (except memory limitations) to the number of backup tunnels that can protect a given interface. A backup tunnel is scalable because it can protect multiple LSPs and multiple interfaces.</td>
</tr>
<tr>
<td></td>
<td>12.0(22)S</td>
<td>• Backup bandwidth protection allows a priority to be assigned to backup tunnels for LSPs carrying certain kinds of data (such as voice).</td>
</tr>
<tr>
<td></td>
<td>12.0(23)S</td>
<td>• Fast Tunnel Interface Down detection, which forces a &quot;generic&quot; interface tunnel (not specifically a Fast Reroute tunnel) to become disabled immediately if the headend router detects a failed link on an LSP.</td>
</tr>
<tr>
<td></td>
<td>12.0(24)S</td>
<td>• Resource Reservation Protocol (RSVP) Hellos, which are used to accelerate the detection of node failures.</td>
</tr>
<tr>
<td></td>
<td>12.0(29)S</td>
<td>In 12.0(10)ST, Fast Reroute Link Protection feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.0(30)S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td>In 12.0(16)ST, Link Protection for Cisco series 7200 and 7500 platforms was added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 12.0(22)S, Fast Reroute enhancements were added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 12.0(23)S, the <code>show mpls traffic-eng fast-reroute database</code> command was revised.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 12.0(24)S, support for the Cisco 10720 Internet router and the Cisco 12000 series router engine 3 was added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 12.0(29)S, backup bandwidth protection was added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In 12.0(30)S, support for the following was added:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Node Protection Desired, Fast Tunnel Interface Down Detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fast Reroute over ATM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Gigabit Ethernet line cards</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Link protection for GE interfaces on 10x1G engine 4+ GE, 1x10G engine 4+ GE, and 4x1G engine 3 GE routers with the Loss of Signal Fast Reroute trigger</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The <code>tunnel mpls traffic-eng interface down delay</code> command was added.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This feature was integrated into Cisco IOS Release 12.2(33)SRB.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This feature was integrated into Cisco IOS Release 12.4(20)T.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In Cisco IOS Release 15.4(1)S, support was added for the Cisco 901S platform.</td>
<td></td>
</tr>
</tbody>
</table>

In Cisco IOS Release 15.4(1)S,
Glossary

**backup bandwidth** -- The usage of NHOP and NNHOP backup tunnels to provide bandwidth protection for rerouted LSPs.

**backup tunnel** -- An MPLS TE tunnel used to protect other (primary) tunnels’ traffic when a link or node failure occurs.

**bandwidth** -- The available traffic capacity of a link.

**Cisco Express Forwarding** -- A means for accelerating the forwarding of packets within a router, by storing route lookup.

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

**Fast Reroute** -- Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

**global pool** -- The total bandwidth allocated to an MPLS traffic engineering link or node.

**headend** -- The router that originates and maintains a given LSP. This is the first router in the LSP's path.

**hop** -- Passage of a data packet between two network nodes (for example, between two routers).

**instance** -- A Hello instance implements the RSVP Hello extensions for a given router interface address and remote IP address. Active Hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active Hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**interface** -- A network connection.

**Intermediate System-to-Intermediate System** -- IS-IS. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

**link** -- A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**limited backup bandwidth** -- Backup tunnels that provide bandwidth protection.

**load balancing** -- A configuration technique that shifts traffic to an alternative link if a certain threshold is exceeded on the primary link. Load balancing is similar to redundancy in that if an event causes traffic to shift directions, alternative equipment must be present in the configuration. In load balancing, the alternative equipment is not necessarily redundant equipment that operates only in the event of a failure.

**LSP** -- label-switched path. A connection between two routers in which MPLS forwards the packets.

**merge point** -- The backup tunnel’s tail.

**MPLS** -- Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**MPLS global label allocation** -- There is one label space for all interfaces in the router. For example, label 100 coming in one interface is treated the same as label 100 coming in a different interface.

**NHOP** -- next hop. The next downstream node along an LSP’s path.
**NHOP backup tunnel** --next-hop backup tunnel. Backup tunnel terminating at the LSP’s next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

**NNHOP** --next-next hop. The node after the next downstream node along an LSP’s path.

**NNHOP backup tunnel** --next-next-hop backup tunnel. Backup tunnel terminating at the LSP’s next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.

**node** --Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.

**OSPF** --Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**primary LSP** --The last LSP originally signaled over the protected interface before the failure. The primary LSP is the LSP before the failure.

**primary tunnel** --Tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

**promotion** --Conditions, such as a new backup tunnel comes up, cause a reevaluation of a backup tunnel that was chosen for an LSP. If the reevaluation is successful, it is called a promotion.

**protected interface** --An interface that has one or more backup tunnels associated with it.

**redundancy** --The duplication of devices, services, or connections so that, in the event of a failure, the redundant devices, services, or connections can perform the work of those that failed.

**RSVP** --Resource Reservation Protocol. A protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

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

**SRLG** --shared risk link group. Sets of links that are likely to go down together.

**state** --Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**sub-pool** --The more restrictive bandwidth in an MPLS traffic engineering link or node. The subpool is a portion of the link or node’s overall global pool bandwidth.

**tailend** --The router upon which an LSP is terminated. This is the last router in the LSP’s path.

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

**tunnel** --Secure communications path between two peers, such as two routers.

**unlimited backup bandwidth** --Backup tunnels that provide no bandwidth (best-effort) protection (that is, they provide best-effort protection).
CHAPTER 3

MPLS Traffic Engineering (TE) Path Protection

The MPLS Traffic Engineering (TE): Path Protection feature provides an end-to-end failure recovery mechanism (that is, full path protection) for Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

• Finding Feature Information, page 87
• Prerequisites for MPLS Traffic Engineering (TE) Path Protection, page 87
• Restrictions for MPLS Traffic Engineering (TE) Path Protection, page 88
• Information About MPLS Traffic Engineering (TE) Path Protection, page 88
• How to Configure MPLS Traffic Engineering (TE) Path Protection, page 90
• Configuration Examples for MPLS Traffic Engineering (TE): Regular Path Protection, page 103
• Configuration Examples for MPLS Traffic Engineering (TE): Enhanced Path Protection, page 108
• Additional References, page 113
• Feature Information for MPLS Traffic Engineering (TE): Path Protection, page 115
• Glossary, page 117

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 (TE) Path Protection

• Ensure that your network supports MPLS TE, Cisco Express Forwarding, and Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF).
• Enable MPLS.
• Configure TE on the routers.
• Configure a TE tunnel with a primary path option by using the `tunnel mpls traffic-eng path-option` command.
• If your router supports SSO, configure Resource Reservation Protocol (RSVP) Graceful Restart in full mode on the routers.
• If your router supports SSO, for NSF operation you must have configured SSO on the device.

Restrictions for MPLS Traffic Engineering (TE) Path Protection

• There can be only one secondary path for each primary path option.
• The secondary path will not be signaled with the Fast Reroute (FRR) flag.
• Dynamic diverse paths are not supported.
• Do not use link and node protection with path protection on the headend router.
• Do not configure path protection on an automesh tunnel template because the destinations are different and you cannot use the same path option to reach multiple destinations.
• A lockdown option is not supported in protected path options.
• After an SSO event, path protection will not be immediately available on tunnels. Only a single label switched path (LSP) is checkpointed and recovered for the tunnel; the path-protected LSP will not be signaled until the end of the RSVP High Availability (HA) recovery period.

Information About MPLS Traffic Engineering (TE) Path Protection

Traffic Engineering Tunnels

MPLS TE lets you build label switched paths (LSPs) across your network for forwarding traffic. MPLS TE LSPs, also called TE tunnels, let the headend of a TE tunnel control the path its traffic takes to a particular destination. This method is more flexible than forwarding traffic based only on a destination address. Some tunnels are more important than others. For example, you may have tunnels carrying VoIP traffic and tunnels carrying data traffic that are competing for the same resources. MPLS TE allows you to have some tunnels preempt others. Each tunnel has a priority, and more-important tunnels take precedence over less-important tunnels.

Path Protection

Path protection provides an end-to-end failure recovery mechanism (that is, full path protection) for MPLS TE tunnels. A secondary LSP is established, in advance, to provide failure protection for the protected LSP that is carrying a tunnel’s TE traffic. When there is a failure on the protected LSP, the headend router immediately enables the secondary LSP to temporarily carry the tunnel’s traffic. If there is a failure on the
secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared. Path protection can be used with a single area (OSPF or IS-IS), or Inter-AS (Border Gateway Protocol (BGP), external BGP (eBGP), and static).

The failure detection mechanisms that trigger a switchover to a secondary tunnel include the following:

- Path error or resv tear from Resource Reservation Protocol (RSVP) signaling
- Notification from the RSVP hello that a neighbor is lost
- Notification from the Bidirectional Forwarding Detection (BFD) protocol that a neighbor is lost
- Notification from the Interior Gateway Protocol (IGP) that the adjacency is down
- Local teardown of the protected tunnel’s LSP due to preemption in order to signal higher priority LSPs, a Packet over SONET (POS) alarm, online insertion and removal (OIR), and so forth

An alternate recovery mechanism is Fast Reroute (FRR), which protects MPLS TE LSPs only from link and node failures by locally repairing the LSPs at the point of failure.

Although not as fast as link or node protection, presignaling a secondary LSP is faster than configuring a secondary primary path option or allowing the tunnel’s headend router to dynamically recalculate a path. The actual recovery time is topology-dependent, and affected by delay factors such as propagation delay or switch fabric latency.

**Enhanced Path Protection**

Enhanced path protection provides support of multiple backup path options per primary path option. You can configure up to eight backup path options for a given primary path option. Only one of the configured backup path options is actively signaled at any time.

After you enter the `mpls traffic-eng path-option list` command, you can enter the backup path priority in the `number` argument of the `path-option` command. A lower identifier represents a higher priority. Priorities are configurable for each backup path option. Multiple backup path options and a single backup path option cannot coexist to protect a primary path option.

**ISSU**

Cisco ISSU allows you to perform a Cisco IOS XE software upgrade or downgrade while the system continues to forward packets. ISSU takes advantage of the Cisco IOS XE high availability infrastructure--Cisco NSF with SSO and hardware redundancy--and eliminates downtime associated with software upgrades or version changes by allowing changes while the system remains in service. That lowers the impact that planned maintenance activities have on network service availability; there is less downtime and better access to critical systems.

When Path Protection is enabled and an ISSU upgrade is performed, path protection performance is similar to other TE features.

**NSF/SSO**

Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure.
SSO takes advantage of Route Processor (RP) redundancy to increase network availability by establishing one of the RPs as the active processor while the other RP is designated as the secondary processor, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them. A switchover from the active to the secondary processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Cisco NSF works with SSO to minimize the amount of time a network is unavailable to users after a switchover. The main purpose of NSF is to continue forwarding IP packets after an RP switchover. Cisco NSF helps to suppress routing flaps in SSO-enabled devices, thus reducing network instability.

The MPLS Traffic Engineering: Path Protection feature can recover after SSO. A tunnel configured for path protection may have two LSPs signaled simultaneously: the primary LSP that is carrying the traffic and the secondary LSP that carries traffic in case there is a failure along the primary path. Only information associated with one of those LSPs, the one that is currently carrying traffic, is synched to the standby RP. The standby RP, upon recovery, can determine from the checkpointed information whether the LSP was the primary or secondary.

If the primary LSP was active during the switchover, only the primary LSP is recovered. The secondary LSP that was signaled and that provided path protection is resignaled after the TE recovery period is complete. This does not impact traffic on the tunnel because the secondary LSP was not carrying traffic.

How to Configure MPLS Traffic Engineering (TE) Path Protection

Regular Path Protection Configuration Tasks

This section contains the following tasks which are shown in the figure below.

Figure 16: Network Topology--Path Protection

Configuring Explicit Paths for Secondary Paths

To specify a secondary path that does not include common links or nodes associated with the primary path in case those links or nodes go down, configure an explicit path by performing the following steps.
### SUMMARY STEPS

1. enable  
2. configure terminal  
3. ip explicit-path \{name path-name| identifier number\} [enable | disable]  
4. index index command ip-address  
5. exit  
6. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** enable | Enables privileged EXEC mode.  
  • Enter your password if prompted.  
  **Example:**  
  Router> enable |
| **Step 2** configure terminal | Enters global configuration mode.  
  **Example:**  
  Router# configure terminal |
| **Step 3** ip explicit-path \{name path-name| identifier number\} [enable | disable] | Creates or modifies the explicit path and enters IP explicit path command mode.  
  **Example:**  
  Router(config)# ip explicit-path name path3441 enable |
| **Step 4** index index command ip-address | Inserts or modifies a path entry at a specific index. The IP address represents the node ID.  
  **Note** Enter this command once for each router.  
  **Example:**  
  Router(cfg-ip-exp1-path)# index 1 next-address 10.0.0.1 |
| **Step 5** exit | Exits IP explicit path command mode and enters global configuration mode.  
  **Example:**  
  Router(cfg-ip-exp1-path)# exit |
| **Step 6** exit | Exits global configuration mode and enters privileged EXEC mode.  
  **Example:**  
  Router(config)# exit |
Assigning a Secondary Path Option to Protect a Primary Path Option

Assign a secondary path option in case there is a link or node failure along a path and all interfaces in your network are not protected.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface tunnel  number
4. tunnel mpls traffic-eng path-option protect  number  explicit  {name path-name | identifier path-number} [verbatim] [attributes string] [bandwidth kb/s] sub-pool kb/s
5. exit
6. exit

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | enable | Enables privileged EXEC mode.  
• Enter your password if prompted.  

Example:  
Router> enable |
| Step 2 | configure terminal | Enters global configuration mode.  

Example:  
Router# configure terminal |
| Step 3 | interface tunnel  number | Configures a tunnel interface and enters interface configuration mode.  

Example:  
Router(config)# interface tunnel500 |
| Step 4 | tunnel mpls traffic-eng path-option protect  number  explicit  {name path-name | identifier path-number} [verbatim] [attributes string] [bandwidth kb/s] sub-pool kb/s | Configures a secondary path option for an MPLS TE tunnel.  

Example:  
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344 |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits interface configuration mode and returns to global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# exit</td>
</tr>
</tbody>
</table>

| **Step 6** |  |
| exit | Exits global configuration mode and returns to privileged EXEC mode. |
| Example: | Router(config)# exit |

### Verifying the Configuration of MPLS Traffic Engineering Path Protection

To verify the configuration of path protection, perform the following steps. In Steps 1 and 2, refer to the figure below.

**Figure 17: Network Topology Verification**

![Network Topology Verification Diagram]

- Primary path
- Secondary path

**SUMMARY STEPS**

1. `show running interface tunnel tunnel-number`
2. `show mpls traffic-eng tunnels tunnel-interface`
3. `show mpls traffic-eng tunnels tunnel-interface [brief] protection`
4. `show ip rsvp high-availability database {hello | link-management {interfaces | system} | lsp [filter destination ip-address] | filter lsp-id lsp-id | filter source ip-address | filter tunnel-id tunnel-id} | lsp-head [filter number] | summary}`
DETAILED STEPS

Step 1  show running interface tunnel tunnel-number
This command shows the configuration of the primary path and protection path options.

Note  To show the status of both LSPs (that is, both the primary path and the protected path), use the show mpls traffic-eng tunnels protection command.

Example:

Router# show running interface tunnel500
Building configuration...
Current configuration : 497 bytes
!
interface Tunnel500
  ip unnumbered Loopback0
tunnel destination 10.0.0.9
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng path-option 10 explicit name path344
tunnel mpls traffic-eng path-option 20 explicit name path345
tunnel mpls traffic-eng path-option protect 10 explicit name path3441
  tunnel mpls traffic-eng path-option protect 20 explicit name path348
end

Step 2  show mpls traffic-eng tunnels tunnel-interface
This command shows tunnel path information.

The Common Link(s) field shows the number of links shared by both the primary and secondary paths, from the headend router to the tailend router.

The Common Node(s) field shows the number of nodes shared by both the primary and secondary paths, excluding the headend and tailend routers.

As shown in the following output, there are no common links or nodes:

Example:

Router# show mpls traffic-eng tunnels tunnel500
Name: R1 t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
Config Parameters:
  Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : FastEthernet1/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19
    RSVP Path Info:
      My Address: 10.2.0.1
Explicit Route: 10.2.0.2 10.10.0.1 10.0.0.9
Record Route: NONE
Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
Record Route: NONE
Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 10.2.0.1 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
History:
Tunnel:
Time since created: 11 minutes, 17 seconds
Time since path change: 8 minutes, 5 seconds
Number of LSP IDs (Tun_Instances) used: 19
Current LSP:
Uptime: 8 minutes, 5 seconds

Step 3  
use mpls traffic-eng tunnels tunnel Interface [brief] protection
Use this command, with the protection keyword specified, to show the status of both LSPs (that is, both the primary path and the protected path).

Note  Deleting a primary path option has the same effect as shutting down a link. Traffic will move to the protected path in use.
The following command output shows that the primary LSP is up, and the secondary LSP is up and providing protection:

Example:

Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 19
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.2.0.1 10.2.0.2
  10.10.0.1 10.10.0.2
  10.0.0.9
Protect lsp path:10.0.0.1 10.0.0.2
  10.0.1.1 10.0.1.2
  10.0.0.9
Path Protect Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : FastEthernet0/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 27
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

The following command output shows that the primary LSP is down, and the secondary LSP is up and is actively carrying traffic:

Example:

Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 27
Fast Reroute Protection: None
Path Protection: Backup lsp in use.

**Step 4**
```
show ip rsvp high-availability database {hello | link-management {interfaces | system} | lsp [filter destination ip-address] | filter lsp-id lsp-id] | filter source ip-address | filter tunnel-id tunnel-id] | lsp-head [filter number] | summary}
```
The `show ip rsvp high-availability database` command displays the contents of the RSVP high availability (HA) read and write databases used in TE. If you specify the `lsp-head` keyword, the command output includes path protection information.

**Example:**
```
Router# show ip rsvp high-availability database lsp-head
LSP HEAD WRITE DB
Tun ID: 500
Header:
  State: Checkpointed Action: Add
  Seq #: 3 Flags: 0x0
Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10.0.0.1
  RRR path setup info
    Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
    Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
    Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
    Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
    Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
    Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0
```

---

**Enhanced Path Protection Configuration Tasks**

This section contains the following tasks which are shown in the figure below.

**Figure 18: Network Topology - Enhanced Path Protection**

![Network Topology Diagram](image-url)
Creating a Path Option List

Perform the following task to create a path option list of backup paths for a primary path option.

Note
To use a secondary path instead, perform the steps in the Configuring Explicit Paths for Secondary Paths section.

SUMMARY STEPS

1. enable
2. configure terminal
3. mpls traffic-eng path-option list [name pathlist-name | identifier pathlist-number]
4. path-option number explicit [name pathoption-name | identifier pathoption-number]
5. list
6. no [pathoption-name | pathoption-number]
7. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mpls traffic-eng path-option list [name pathlist-name</td>
<td>identifier pathlist-number]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# mpls traffic-eng path-option list name pathlist-01</td>
<td>• You can enter the following commands: path-option, list, no, and exit.</td>
</tr>
<tr>
<td><strong>Step 4</strong> path-option number explicit [name pathoption-name</td>
<td>identifier pathoption-number]</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(cfg-pathoption-list)# path-option 10 explicit identifier 200</td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5 list</td>
<td>(Optional) Lists all of the path options.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-pathoption-list)# list</td>
<td></td>
</tr>
<tr>
<td>Step 6 no [pathoption-name</td>
<td>pathoption-number]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-pathoption-list)# no 10</td>
<td></td>
</tr>
<tr>
<td>Step 7 exit</td>
<td>(Optional) Exits path-option list configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-pathoption-list)# exit</td>
<td></td>
</tr>
</tbody>
</table>

### Assigning a Path Option List to Protect a Primary Path Option

Assign a path option list in case there is a link or node failure along a path and all interfaces in your network are not protected. See the third figure above.

### SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. tunnel mpls traffic-eng path-option protect number [attributes lsp-attributes | bandwidth {kbps | subpool kbps} | explicit {identifier path-number | name path-name} | list {pathlist-name name | identifier pathlist-identifier}]
5. exit

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 3</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>interface tunnel number</td>
<td>Configures a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# interface tunnel500</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 4</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tunnel mpls traffic-eng path-option protect number [attributes lsp-attributes</td>
<td>Configures a path option list to protect primary path option 10.</td>
</tr>
<tr>
<td></td>
<td>bandwidth {kbps</td>
<td>explicit {identifier path-number</td>
</tr>
<tr>
<td></td>
<td>subpool kbps}</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name pathlist-01</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>exit</td>
<td>(Optional) Exits interface configuration mode and enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)# exit</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the Configuration of MPLS Traffic Engineering Path Protection

To verify the configuration of path protection, perform the following steps. In Steps 1 and 2, refer to the figure below.

Figure 19: Network Topology Verification

SUMMARY STEPS

1. show running interface tunnel tunnel-number
2. show mpls traffic-eng tunnels tunnel-interface
3. show mpls traffic-eng tunnels tunnel-interface [brief] protection
4. show ip rsvp high-availability database {hello | link-management {interfaces | system} | lsp [filter destination ip-address] | filter lsp-id lsp-id] | filter source ip-address | filter tunnel-id tunnel-id] | lsp-head [filter number] | summary}

DETAILED STEPS

Step 1 show running interface tunnel tunnel-number
This command shows the configuration of the primary path and protection path options.

Note To show the status of both LSPs (that is, both the primary path and the protected path), use the show mpls traffic-eng tunnels protection command.

Example:

Router# show running interface tunnel500
Building configuration...
Current configuration : 497 bytes
!
interface Tunnel500
  ip unnumbered Loopback0
tunnel destination 10.0.0.9
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng priority 7 7
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng path-option 10 explicit name path344
tunnel mpls traffic-eng path-option 20 explicit name path345
tunnel mpls traffic-eng path-option protect 10 explicit name path3441
tunnel mpls traffic-eng path-option protect 20 explicit name path348
end

Step 2  show mpls traffic-eng tunnels tunnel-interface
This command shows tunnel path information.

The Common Link(s) field shows the number of links shared by both the primary and secondary paths, from the headend router to the tailend router.

The Common Node(s) field shows the number of nodes shared by both the primary and secondary paths, excluding the headend and tailend routers.

As shown in the following output, there are no common links or nodes:

Example:

Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
Config Parameters:
  Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
  InLabel : - OutLabel : FastEthernet1/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19
  RSVP Path Info:
    My Address: 10.2.0.1
    Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.2.0.1 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
History:
  Tunnel:
    Time since created: 11 minutes, 17 seconds
    Time since path change: 8 minutes, 5 seconds
  Number of LSP IDs (Tun_Instances) used: 19
  Current LSP:
    Uptime: 8 minutes, 5 seconds

Step 3  show mpls traffic-eng tunnels tunnel-interface [brief] protection
Use this command, with the `protection` keyword specified, to show the status of both LSPs (that is, both the primary path and the protected path).

**Note** Deleting a primary path option has the same effect as shutting down a link. Traffic will move to the protected path in use.

The following command output shows that the primary LSP is up, and the secondary LSP is up and providing protection:

**Example:**

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 19
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path: 10.2.0.1  10.2.0.2
  10.10.0.1 10.10.0.2
  10.0.0.9
  Protect lsp path: 10.0.0.1  10.0.0.2
  10.0.1.1 10.0.1.2
  10.0.0.9
  Path Protect Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 27
  RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
    RSVP Resv Info:
      Record Route: NONE
      Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
```

The following command output shows that the primary LSP is down, and the secondary LSP is up and is actively carrying traffic:

**Example:**

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 27
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
```

**Step 4**

```
show ip rsvp high-availability database \{hello \| link-management \{interfaces \| system\} \| lsp \[filter destination ip-address\] \[filter lsp-id lsp-id\] \[filter source ip-address\] \[filter tunnel-id tunnel-id\]\} \[lsp-head \[filter number\]\] \| summary\}
```

The `show ip rsvp high-availability database` command displays the contents of the RSVP high availability (HA) read and write databases used in TE. If you specify the `lsp-head` keyword, the command output includes path protection information.

**Example:**

```
Router# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
Tun ID: 500
Header:
  State: Checkpointed  Action: Add
```
Configuration Examples for MPLS Traffic Engineering (TE): Regular Path Protection

Example Configuring Explicit Paths for Secondary Paths

The figure below illustrates a primary path and a secondary path. If there is a failure, the secondary path is used.

**Figure 20: Primary Path and Secondary Path**

![Diagram of a primary and secondary path]

In the following example the explicit path is named path3441. There is an index command for each router. If there is failure, the secondary path is used.

```
Router(config)# ip explicit-path name path3441 enable
Router(cfg-ip-expl-path)# index 1 next 10.0.0.1
Explicit Path name path3441:
  1: next-address 10.0.0.1
```
Example Assigning a Secondary Path Option to Protect a Primary Path Option

In the following example a traffic engineering tunnel is configured:

Router> enable
Router# configure terminal
Router(config-if)# interface tunnel500
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344

The following show running interface command output shows that path protection has been configured. Tunnel 500 has path option 10 using path344 and protected by path 3441, and path option 20 using path345 and protected by path348.

Router# show running interface tunnel500
Router# interface tunnel 500
Building configuration...
Current configuration : 497 bytes

  interface Tunnel500
    ip unnumbered Loopback0
    tunnel destination 10.0.0.9
    tunnel mode mpls traffic-eng
    tunnel mpls traffic-eng autoroute announce
    tunnel mpls traffic-eng priority 7 7
    tunnel mpls traffic-eng bandwidth 100
    tunnel mpls traffic-eng path-option 10 explicit name path344
    tunnel mpls traffic-eng path-option 20 explicit name path345
    tunnel mpls traffic-eng path-option protect 10 explicit name path3441
    tunnel mpls traffic-eng path-option protect 20 explicit name path348
end

Example Configuring Tunnels Before and After Path Protection

The show mpls traffic-eng tunnels command shows information about the primary (protected) path. The following sample output shows that path protection has been configured.

Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500  (Tunnel500)  Destination: 10.0.0.9
Status:
  Admin: up  Oper: up  Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
Config Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based auto-bw: disabled
Active Path Option Parameters:
State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : FastEthernet1/0/0, 16
RSVP Signalling Info:
Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 43
RSVP Path Info:
My Address: 10.2.0.1
Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
Record Route: NONE
Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
Record Route: NONE
Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
Tunnel:
Time since created: 18 minutes, 22 seconds
Time since path change: 19 seconds
Number of LSP IDs (Tun_Instances) used: 43
Current LSP:
Uptime: 22 seconds
Selection: reoptimization
Prior LSP:
ID: path option 10 [27]
Removal Trigger: reoptimization completed

The following show mpls traffic-eng tunnels command output shows information about the secondary path. Tunnel500 is protected. The protection path is used, and the primary path is down. The command output shows the IP explicit paths of the primary LSP and the secondary LSP.

Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 43
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.2.0.1 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
Protect lsp path:10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
Path Protect Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : FastEthernet0/0/0, 17
RSVP Signalling Info:
Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
RSVP Path Info:
My Address: 10.0.0.1
Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
Record Route: NONE
Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
Record Route: NONE
Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
The following `shutdown` command shuts down the interface to use path protection:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# shutdown
Router(config-if)# end
```

The following `show mpls traffic-eng tunnels` command shows that the protection path is used, and the primary path is down:

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
    Admin: up Oper: up Path: valid Signalling: connected
    path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
    path option 10, type explicit path344
    path protect option 20, type explicit path345
    Path Protection: Backup lsp in use.
    path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
    path protect option 20, type explicit path348

Config Parameters:
    Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
    auto-bw: disabled

Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

OutLabel : FastEthernet0/0/0, 17
RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
    RSVP Resv Info:
        Record Route: NONE
        Pspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
    Shortest Unconstrained Path Info:
        Path Weight: 20 (TE)
    Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9

History:
    Tunnel:
        Time since created: 23 minutes, 28 seconds
        Time since path change: 50 seconds
    Number of LSP IDs (Tun_Instances) used: 44
    Current LSP:
        Uptime: 5 minutes, 24 seconds
    Selection:
    Prior LSP:
        ID: path option 10 [43]
        Removal Trigger: path error
        Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
```

The "up" value in the Oper field of the `show mpls traffic-eng tunnels protection` command shows that protection is enabled:

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 44
Fast Reroute Protection: None
```
Path Protection: Backup lsp in use.
R1#

The no shutdown command in the following command sequence causes the interface to be up again and activates the primary path:

Router> enable

Router# configure terminal

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

Router(config)# interface fastethernet1/0/0

Router(config-if)# no shutdown

Router(config-if)# end

The following command output shows that path protection has been reestablished and the primary path is being used:

Router# show mpls traffic-eng tunnels tunnel500

Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path346
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348

Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled

Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel :
OutLabel : FastEthernet1/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
RSVP Path Info:
  My Address: 10.2.0.1
  Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
  Tunnel:
    Time since created: 25 minutes, 26 seconds
    Time since path change: 23 seconds
    Number of LSP IDs (Tun_Instances) used: 52
  Current LSP:
    Uptime: 26 seconds
    Selection: reoptimization
    Prior LSP:
      ID: path option 10 [44]
      Removal Trigger: reoptimization completed

R1#

Following is sample show mpls traffic-eng tunnels command output. Tunnel500 is protected. After a failure, the primary LSP is protected.

Router# show mpls traffic-eng tunnels tunnel500 protection

R1 t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 52

MPLS Traffic Engineering Path, Link, and Node Protection Configuration Guide, Cisco IOS Release 15M&T
Configuration Examples for MPLS Traffic Engineering (TE): Enhanced Path Protection

Creating a Path Option List: Example

The figure below shows the network topology for enhanced path protection.

The following example configures two explicit paths named secondary1 and secondary2.

Router(config)# ip explicit-path name secondary1
In the following example a path option list of backup paths is created. You define the path option list by using the explicit paths.

Assigning a Path Option List to Protect a Primary Path Option: Example

In the following example, a traffic engineering tunnel is configured:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface tunnel 2
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name secondary-list

The following show running interface command output shows that path protection has been configured. Tunnel 2 has path option 10 using path primary1 and protected by secondary-list.

Router# show running-config interface tunnel 2
Building configuration...
Current configuration : 296 bytes
!
interface Tunnel2
  ip unnumbered Loopback0
tunnel mode mpls traffic-eng
tunnel destination 103.103.103.103
tunnel mpls traffic-eng autорoute announce
tunnel mpls traffic-eng path-option 10 explicit name primary1
tunnel mpls traffic-eng path-option protect 10 list name secondary-list
Example Configuring Tunnels Before and After Path Protection

The `show mpls traffic-eng tunnels` command shows information about the primary (protected) path. The following sample output shows that path protection has been configured.

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500)  Destination: 10.0.0.9
Status:
  Admin: up  Oper: up  Path: valid  Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
Config Parameters:
  Bandwidth: 100 kbps (Global)  Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled  LockDown: disabled  Loadshare: 100 bw-based
  auto-bw: disabled
Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled
  InLabel : -
  OutLabel : FastEthernet1/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dat 10.0.0.9, Tun_Id 500, Tun_Instance 43
RSVP Path Info:
  My Address: 10.2.0.1
  Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
  Tunnel:
    Time since created: 18 minutes, 22 seconds
    Time since path change: 19 seconds
    Number of LSP IDs (Tun_Instances) used: 43
  Current LSP:
    Uptime: 22 seconds
    Selection: reoptimization
    Prior LSP:
    ID: path option 10 [27]
    Removal Trigger: reoptimization completed
```

The following `show mpls traffic-eng tunnels` command output shows information about the secondary path. Tunnel500 is protected. The protection path is used, and the primary path is down. The command output shows the IP explicit paths of the primary LSP and the secondary LSP.

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 43
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path: 10.2.0.1 10.2.0.2 10.0.0.9
  Protect lsp path: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
```
Path Protect Parameters:
- Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
- Metric Type: TE (default)
- InLabel : -
- OutLabel : FastEthernet0/0/0, 17
- RSVP Signalling Info:
  - Src 10.0.0.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
  - RSVP Path Info:
    - My Address: 10.0.0.1
    - Explicit Route: 10.0.0.2 10.0.0.9 10.0.0.1 10.0.0.2
    - Record Route: NONE
    - Tspe: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
    - RSVP Resv Info:
      - Record Route: NONE
      - Fspe: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

The following `shutdown` command shuts down the interface to use path protection:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# shutdown
Router(config-if)# end
Router#

The following `show mpls traffic-eng tunnels` command shows that the protection path is used, and the primary path is down:

Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel1500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
    InLabel : -
    OutLabel : FastEthernet0/0/0, 17
  RSVP Signalling Info:
    Src 10.0.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
    RSVP Path Info:
      My Address: 10.0.0.1
      Explicit Route: 10.0.0.2 10.0.0.1 10.0.0.2 10.0.0.9
      Record Route: NONE
      Tspe: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
      RSVP Resv Info:
        Record Route: NONE
        Fspe: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 20 (TE)
    Explicit Route: 10.0.0.1 10.0.0.2 10.0.0.9 10.0.0.1 10.0.0.2
    History:
      Tunnel:
      Time since created: 23 minutes, 28 seconds
      Time since path change: 50 seconds
      Number of LSP IDs (Tun_Instances) used: 44
      Current LSP:
        Uptime: 5 minutes, 24 seconds
        Selection:
        Prior LSP:
ID: path option 10 [43]
Removal Trigger: path error
Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1

The "up" value in the Oper field of the `show mpls traffic-eng tunnels protection` command shows that protection is enabled:

```
Router# show mpls traffic-eng tunnels tunnel500 protection
R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 44
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
R1#
```

The `no shutdown` command in the following command sequence causes the interface to be up again and activates the primary path:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet1/0/0
Router(config-if)# no shutdown
Router(config-if)# end
```

The following command output shows that path protection has been reestablished and the primary path is being used:

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
Status:
   Admin: up Oper: up Path: valid Signalling: connected
   path option 10, type explicit path344 (Basis for Setup, path weight 20)
   path option 20, type explicit path345
   Path Protection: 0 Common Link(s), 0 Common Node(s)
   path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
   path protect option 20, type explicit path348
Config Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
   AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
   auto-bw: disabled
Active Path Option Parameters:
   State: explicit path option 10 is active
   BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
   InLabel : -
   OutLabel : FastEthernet1/0/0, 16
RSVP Signalling Info:
   Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
   RSVP Path Info:
      My Address: 10.2.0.1
      Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
      Record Route: NONE
      Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
      Record Route: NONE
      Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   Shortest Unconstrained Path Info:
      Path Weight: 20 (TE)
      Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
   History:
      Tunnel:
         Time since created: 25 minutes, 26 seconds
         Time since path change: 23 seconds
      Number of LSP IDs (Tun_Instances) used: 52
Current LSP:
```
Uptime: 26 seconds
Selection: reoptimization
Prior LSP:
  ID: path option 10 (44)
  Removal Trigger: reoptimization completed

R1# Following is sample show mpls traffic-eng tunnels command output. Tunnel500 is protected. After a failure, the primary LSP is protected.

Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 52
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path: 10.2.0.1 10.2.0.2
  10.10.0.1 10.10.0.2
  10.0.0.9
Protect lsp path: 10.0.0.1 10.0.2
  10.0.1.1 10.0.1.2
  10.0.0.9
Path Protect Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : FastEthernet0/0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dat 10.0.0.9, Tun_Id 500, Tun_Instance 53
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits

R1#

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>Link and node protection</td>
<td>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</td>
</tr>
<tr>
<td>Multiprotocol Label Switching commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>Bidirectional Forwarding Direction configuration information</td>
<td>“Bidirectional Forwarding Detection” chapter in the Cisco IOS IP Routing Configuration Guide</td>
</tr>
</tbody>
</table>
### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

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

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>
Feature Information for MPLS Traffic Engineering (TE): Path Protection

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 (TE): Path Protection

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
</table>
| MPLS Traffic Engineering (TE): Path Protection | 12.0(30)S  
12.2(18)SXD  
12.2(33)SRC  
12.2(33)SRE  
12.2(50)SY  
12.4(20)T | The MPLS Traffic Engineering (TE): Path Protection feature provides an end-to-end failure recovery mechanism (that is, full path protection) for MPLS TE tunnels.  
In Cisco IOS Release 12.0(30)S, this feature was introduced.  
In Cisco IOS Release 12.2(18)SXD, this feature was integrated.  
In Cisco IOS Release 12.2(33)SRC, support was added for In Service Software Upgrade (ISSU) and Cisco nonstop forwarding with stateful switchover (NSF/SSO). The following command was modified by this feature: `show ip rsvp high-availability database`. The following command was added: `tunnel mpls traffic-eng path-option protect`.  
In Cisco IOS Release 12.4(20)T, this feature was integrated. ISSU was not supported, and NSF with SSO was not supported. The following commands were modified: `show ip rsvp high-availability database`, `tunnel mpls traffic-eng path-option`, and `tunnel mpls traffic-eng path-option protect`.  
In Cisco IOS Release 12.2(33)SRE, support was added for enhanced path protection. The following commands were added or modified: `mpls traffic-eng path-option list`, `show mpls traffic-eng path-option list`, `show mpls traffic-eng tunnels`, and `tunnel mpls traffic-eng path-option protect`. |
Glossary

**autotunnel mesh group** -- An autotunnel mesh group (referred to as a mesh group) is a set of connections between edge LSRs in a network.

**backup tunnel** -- An MPLS TE tunnel used to protect other (primary) tunnels' traffic when a link or node failure occurs.

**BGP** -- Border Gateway Protocol. An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).

**Cisco Express Forwarding** -- A means for accelerating the forwarding of packets within a router, by storing route lookup.

**Fast Reroute** -- Procedures that enable temporary routing around a failed link or node while a new LSP is being established at the headend.

**graceful restart** -- A process for helping an RP restart after a node failure has occurred.

**headend** -- The router that originates and maintains a given LSP. This is the first router in the LSP’s path.

**hop** -- Passage of a data packet between two network nodes (for example, between two routers).

**interface** -- A network connection.

**IS-IS** -- Intermediate System-to-Intermediate System. Link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

**ISSU** -- In Service Software Upgrade. The ISSU process allows Cisco IOS XE software at the router level to be updated or otherwise modified while packet forwarding continues.

**link** -- A point-to-point connection between adjacent nodes. There can be more than one link between adjacent nodes. A link is a network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**LSP** -- Label switched path. A configured connection between two routers, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

**MPLS** -- Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

**NHOP** -- next hop. The next downstream node along an LSP’s path.

**NHOP backup tunnel** -- next-hop backup tunnel. The backup tunnel terminating at the LSP’s next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link, and is used to protect primary LSPs that were using this link before the failure.

**NNHOP** -- next-next hop. The node after the next downstream node along an LSP's path.

**NNHOP backup tunnel** -- next-next-hop backup tunnel. The backup tunnel terminating at the LSP’s next-next hop beyond the point of failure, and originating at the hop immediately upstream of the point of failure. It bypasses a failed link or node, and is used to protect primary LSPs that were using this link or node before the failure.

**node** -- The endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network. Nodes can be processors, controllers, or workstations.
NSF -- Cisco nonstop forwarding. Cisco NSF always runs with stateful switchover (SSO) and provides redundancy for Layer 3 traffic. NSF works with SSO to minimize the amount of time that a network is unavailable to its users following a switchover. The main purpose of NSF is to continue forwarding IP packets following a supervisor engine switchover.

OSPF -- Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

primary LSP -- The last LSP originally signaled over the protected interface before the failure. A primary LSP is signaled by configuring a primary path option.

primary tunnel -- A tunnel whose LSP may be fast rerouted if there is a failure. Backup tunnels cannot be primary tunnels.

protected interface -- An interface that has one or more backup tunnels associated with it.

router -- A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

RP -- Route Processor. A generic term for the centralized control unit in a chassis.

RSVP -- Resource Reservation Protocol. An IETF protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

secondary LSP -- The LSP that is signaled to provide path protection. A secondary LSP protects a primary LSP.

secondary path option -- Configuration of the path option that provides protection.

SRLG -- Shared Risk Link Group. Sets of links that are likely to go down together (for example, because they have the same underlying fiber).

state -- Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

tailend -- The router upon which an LSP is terminated. This is the last router in the LSP's path.

TE -- traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

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

tunnel -- Secure communications path between two peers, such as two routers.

VoIP -- Voice over IP. The capability of a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. Cisco's voice support is implemented by using voice packet technology.
MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

The MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for Multiprotocol Label Switching (MPLS) TE label switched path (LSP).

The feature is enabled through the `ip explicit-path` command that allows you to create an IP explicit path and enter a configuration submode for specifying the path. The feature adds to the submode commands the `exclude-address` command for specifying addresses to exclude from the path.

If the excluded address for an MPLS TE LSP identifies a flooded link, the constraint-based shortest path first (CSPF) routing algorithm does not consider that link when computing paths for the LSP. If the excluded address specifies a flooded MPLS TE router ID, the CSPF routing algorithm does not allow paths for the LSP to traverse the node identified by the router ID.

- Finding Feature Information, page 119
- Prerequisites for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 120
- Restrictions for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 120
- Information About MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 120
- How to Configure MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 121
- Configuration Examples for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 124
- Additional References, page 125
- Feature Information for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion, page 127
- Glossary, page 127

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 (TE)--IP Explicit Address Exclusion

Your network must support the following Cisco IOS features in order to support IP explicit address exclusion:

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

Restrictions for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

MPLS TE will accept an IP explicit path comprised of either all excluded addresses configured by the `exclude-address` command or all included addresses configured by the `next-address` command, but not a combination of both.

Information About MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

MPLS Traffic Engineering

MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

Traffic engineering (TE) is the process of adjusting bandwidth allocations to ensure that enough is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then fixes the bandwidth available for that tunnel.

Cisco Express Forwarding

Cisco Express Forwarding is an advanced, Layer 3 switching technology inside a router. It defines the fastest method by which a Cisco router forwards packets from ingress to egress interfaces. The `ip cef` command enables Cisco Express Forwarding globally, and the `ip route-cache cef` command enables Cisco Express Forwarding on an interface.
How to Configure MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

Configuring IP Explicit Address Exclusion

SUMMARY STEPS

1. enable
2. configure terminal
3. ip explicit-path {name path-name | identifier number} [enable | disable]
4. exclude-address ip-address
5. exit
6. show ip explicit-path

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip explicit-path {name path-name</td>
<td>identifier number} [enable</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip explicit-path name OmitR12</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> exclude-address ip-address</td>
<td>Excludes the specified link or node from consideration by the constraint-based SPF.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(cfg-ip-expl-path)# exclude-address 10.12.12</td>
<td>• The ip-address is a link address or the router ID for a node.</td>
</tr>
</tbody>
</table>
Configuring an MPLS Traffic Engineering Tunnel

SUMMARY STEPS

1. enable
2. configure terminal
3. interface tunnel number
4. ip unnumbered loopback0
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 | ID path-number}}
   [lockdown]
9. exit
10. exit
11. show mpls traffic eng tunnels

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 5</strong> exit</td>
<td>Exits from explicit-path configuration mode, and returns to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 6</strong> show ip explicit-path</td>
<td>Displays information about configured IP explicit paths.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show ip explicit-path</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action | Purpose |
---|---
**Step 2** configure terminal  | Enters global configuration mode. |
Example:  
Router# configure terminal  |
**Step 3** interface tunnel number  | Configures an interface type and enters interface configuration mode. |
Example:  
Router(config)# interface tunnel11  |
**Step 4** ip unnumbered loopback0  | Assigns the tunnel interface an IP address.  
- An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |
Example:  
Router(config-if)# ip unnumbered loopback0  |
**Step 5** tunnel destination ip-address  | Specifies the destination for a tunnel.  
- The destination of the tunnel must be the MPLS traffic engineering router ID of the destination device. |
Example:  
Router(config-if)# tunnel destination 10.11.11.11  |
**Step 6** tunnel mode mpls traffic-eng  | Sets the tunnel encapsulation mode to MPLS traffic engineering. |
Example:  
Router(config-if)# tunnel mode mpls traffic-eng  |
**Step 7** tunnel mpls traffic-eng bandwidth bandwidth  | Configures the bandwidth for the MPLS traffic engineering tunnel. |
Example:  
Router(config-if)# tunnel mpls traffic-eng bandwidth 100  |
**Step 8** tunnel mpls traffic-eng path-option number {dynamic | explicit {name path-name | ID path-number}} [lockdown]  | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.  
- A dynamic path is used if an explicit path is unavailable. |
Example:  
Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic  
**Note** To configure a path option that specifies an exclude address, specify the explicit keyword (not the dynamic keyword) and specify an IP explicit path configured according to the steps in the "Configuring IP Explicit Address Exclusion" section.
### Purpose

**Command or Action**  
**Purpose**

**Step 9**  
*exit*  
**Example:**  
Router(config-if)# exit  

- Exits from interface configuration mode.

**Step 10**  
*exit*  
**Example:**  
Router(config)# exit  

- Exits to privileged EXEC mode.

**Step 11**  
*show mpls traffic eng tunnels*  
**Example:**  
Router# show mpls traffic eng tunnels  

- Shows information about tunnels, including the current tunnel path if a tunnel is operational.
  - By viewing the command output, you can determine the path that was used to build a tunnel. If you entered the `exclude-address` command, the specified link or node should not be listed.

---

## Configuration Examples for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

### Configuring IP Explicit Address Exclusion Example

The following example shows how to configure an MPLS TE tunnel with two path options: a preferred explicit path with an excluded address and a backup dynamic path.

Configure the IP explicit path named `OmitR12`, which excludes the router with router ID 10.12.12.12:

```bash
ip explicit-path name OmitR12  
exclude-address 10.12.12.12  
Explicit Path name OmitR12:  
  1: exclude-address 10.12.12.12  
ext
```

To verify the configuration of the explicit path, use the `show ip explicit-path` command:

```bash
show ip explicit-paths name OmitR12  
PATH OmitR12 (loose source route, path complete, generation 3)  
  1: exclude-address 10.12.12.12
```
You must know the router IDs for LSRs (nodes) in the network; in this example, that 10.12.12.12 is a router ID. Otherwise, it will not be apparent whether the specified address is the IP address of a link or a router ID.

### Configuring an MPLS Traffic Engineering Tunnel Example

The following example configures Tunnel11 with its two options, where the preferred path option is the IP explicit path OmitR2:

```sh
tunnel mpls traffic-eng path-option 1 explicit name OmitR12
```

There are additional commands for configuring properties for TE tunnels such as bandwidth and priority. For descriptions of those commands, refer to the [Cisco IOS IP Switching Services Configuration Guide](#).

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>MPLS traffic engineering commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>RSVP commands</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>IS-IS</td>
<td>- Cisco IOS IP Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>* Configuring a Basic IS-IS Network</td>
</tr>
<tr>
<td>OSPF</td>
<td>- Cisco IOS IP Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>* Configuring OSPF</td>
</tr>
<tr>
<td>ISSU</td>
<td>Cisco IOS XE In Service Software Upgrade Support</td>
</tr>
</tbody>
</table>
### Related Topic

| NSF/SSO                        |  
|-------------------------------|---
|                               |  

### Document Title

- Cisco Nonstop Forwarding
- Stateful Switchover

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF/SSO</td>
<td></td>
</tr>
</tbody>
</table>

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

### MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 software releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

### Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

Feature Information for MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion

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 (TE)--IP Explicit Address Exclusion

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
</table>
| MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion | 12.0(14)ST 12.2(4)T 12.2(4)T2 12.2(14)S 12.0(32)S 12.2(28)SB | The MPLS Traffic Engineering (TE)--IP Explicit Address Exclusion feature provides a means to exclude a link or node from the path for Multiprotocol Label Switching (MPLS) TE label switched path (LSP).
|                                                 |                   | The following command was introduced by this feature: `exclude-address`.
|                                                 |                   | In 12.0(14)ST, this feature was introduced.
|                                                 |                   | In 12.2(4)T, this feature was integrated into Release 12.2(4)T.
|                                                 |                   | In 12.2(4)T2, this feature was integrated into Release 12.2(4)T2.
|                                                 |                   | In 12.2(14)S, this feature was integrated into Release 12.2(14)S.
|                                                 |                   | In 12.0(32)S, this feature was integrated into Release 12.0(32)S.
|                                                 |                   | In 12.2(28)SB, this feature was integrated into Release 12.2(28)SB.

Glossary

**CEF** --Cisco express forwarding. A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**IP explicit path** --A list of IP addresses, each representing a node or link in the explicit path.
**link** -- Network communications channel consisting of a circuit or transmission path and all related equipment between a sender and a receiver. Sometimes referred to as a line or a transmission link.

**MPLS** -- Multiprotocol Label Switching. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

**node** -- Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.
MPLS Traffic Engineering-Autotunnel Primary and Backup

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

A router with primary one-hop autotunnels and backup autotunnels can be configured with stateful switchover (SSO) redundancy.

• Finding Feature Information, page 129
• Prerequisites for MPLS Traffic Engineering-Autotunnel Primary and Backup, page 130
• Restrictions for MPLS Traffic Engineering-Autotunnel Primary and Backup, page 130
• Information About MPLS Traffic Engineering-Autotunnel Primary and Backup, page 130
• How to Configure MPLS Traffic Engineering Autotunnel Primary and Backup, page 137
• Configuration Examples for MPLS Traffic Engineering-Autotunnel Primary and Backup, page 140
• Additional References, page 144
• Feature Information for MPLS Traffic Engineering-Autotunnel Primary and Backup, page 146
• Glossary, page 148

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 Primary and Backup

- Configure TE on the routers.

Restrictions for MPLS Traffic Engineering-Autotunnel Primary and Backup

- You cannot configure a static route to route traffic over TE autotunnels. For autotunnels, you should use only the autoroute for tunnel selection.

Information About MPLS Traffic Engineering-Autotunnel Primary and Backup

Overview of MPLS Traffic Engineering-Autotunnel Primary and Backup

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature has the following features:

- Backup autotunnel-Enables a router to dynamically build backup tunnels.
- Primary one-hop autotunnel-Enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

If no backup tunnels exist, the following types of backup tunnels are created:

- Next hop (NHOP)
- Next-next hop (NNHOP)

Benefits of MPLS Traffic Engineering-Autotunnel Primary and Backup Feature

- Backup tunnels are built automatically, eliminating the need for users to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface.
- The dynamic creation of one-hop primary tunnels eliminates the need to configure an MPLS TE tunnel with the Fast Reroute (FRR) option for the tunnel to be protected.
- Protection is expanded; FRR does not protect IP traffic that is not using the TE tunnel or Label Distribution Protocol (LDP) labels that are not using the TE tunnel.
MPLS Traffic Engineering

MPLS is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

TE is the process of adjusting bandwidth allocations to ensure that enough bandwidth is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then sets the bandwidth available for that tunnel.

MPLS Traffic Engineering Backup Autotunnels

MPLS backup autotunnels protect fast reroutable TE label switched paths (LSPs). Without MPLS backup autotunnels to protect a LSP you had to do the following:

• Preconfigure each backup tunnel.
• Assign the backup tunnels to the protected interfaces.

An LSP requests backup protection from Resource Reservation Protocol (RSVP) FRR in the following situations:

• Receipt of the first RSVP Resv message
• Receipt of an RSVP path message with the protection attribute after the LSP has been established without the protection attribute
• Detection that a Record Route Object (RRO) changed

If there was no backup tunnel protecting the interface used by the LSP, the LSP remained unprotected.

Backup autotunnels enable a router to dynamically build backup tunnels when they are needed. This prevents you from having to build MPLS TE tunnels statically.

Backup tunnels may not be available for the following reasons:

• Static backup tunnels are not configured.
• Static backup tunnels are configured, but cannot protect the LSP. The backup tunnel may not have enough available bandwidth, the tunnel may protect a different pool, or the tunnel may be down.

If a backup tunnel is not available, the following two backup tunnels are created dynamically:

• NHOP--Protects against link failure
• NNHOP--Protects against node failure

Note
At the penultimate hop, only an NHOP backup tunnel is created.
If two LSPs share the same output interface and NHOP, three (not four) backup tunnels are created. They share an NHOP backup tunnel.

**Link Protection**

Backup tunnels that bypass only a single link of the LSP’s path provide Link Protection. They protect LSPs if a link along their path fails by rerouting the LSP’s traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP’s next hop beyond the point of failure. The figure below illustrates an NHOP backup tunnel.

*Figure 21: NHOP Backup Tunnel*

![NHOP Backup Tunnel Diagram](image)

**Node Protection**

Backup tunnels that bypass next-hop nodes along LSP paths are called NNHOP backup tunnels because they terminate at the node following the next-hop node of the LSPs, thereby bypassing the next-hop node. They protect LSPs by enabling the node upstream of a link or node failure to reroute the LSPs and their traffic around the failure to the next-hop node. NNHOP backup tunnels also provide protection from link failures because they bypass the failed link and the node.
The figure below illustrates an NNHOP backup tunnel.

*Figure 22: Next-Next Hop Backup Tunnel*

![Next-Next Hop Backup Tunnel Diagram]

**Explicit Paths**

Explicit paths are used to create backup autotunnels as follows:

- NHOP excludes the protected link’s IP address.
- NNHOP excludes the NHOP router ID.
- The explicit-path name is `auto-tunnel_tunnelxxx`, where `xxx` matches the dynamically created backup tunnel ID.
- The interface used for the `ip unnumbered` command defaults to Loopback0. You can configure this to use a different interface.

**Range for Backup Autotunnels**

The tunnel range for backup autotunnels is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 1000 to 1100 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the MPLS TE dynamic tunnel software can use those IDs.

**MPLS Traffic Engineering Primary Autotunnels**

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS traffic. The tunnels are created with zero bandwidth. The constraint-based shortest path first (CSPF) is the same as the shortest path first (SPF) when there is zero bandwidth, so the router’s choice of the autorouted one-hop primary tunnel is the
same as if there were no tunnel. Because it is a one-hop tunnel, the encapsulation is tag-implicit (that is, there is no tag header).

Explicit Paths

Explicit paths are used to create autotunnels as follows:

- The explicit path is dynamically created.
- The explicit path includes the IP address for the interface connected to the next hop.
- The explicit-path name is _auto-tunnel_tunnelxxx, where xxx matches the dynamically created one-hop tunnel ID.
- Interfaces used for the \texttt{ip unnumbered} command default to Loopback0. You can configure this to use a different interface.

Range for Autotunnels

The tunnel range is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 100 to 200 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the IDs become available for use by the MPLS TE dynamic tunnel software.

MPLS Traffic Engineering Label-Based Forwarding

Routers receive a packet, determine where it needs to go by examining some fields in the packet, and send it to the appropriate output device. A label is a short, fixed-length identifier that is used to forward packets. A label switching device normally replaces the label in a packet with a new value before forwarding the packet to the next hop. For this reason, the forwarding algorithm is called label swapping. A label switching device, referred to as an LSR, runs standard IP control protocols (that is, routing protocols, RSVP, and so forth) to determine where to forward packets.

Benefits of MPLS Traffic Engineering Protection

The following sections describe the benefits of MPLS traffic engineering protection:

**Delivery of Packets During a Failure**

Backup tunnels that terminate at the NNHOP protect both the downstream link and node. This provides protection for link and node failures.

**Multiple Backup Tunnels Protecting the Same Interface**

In addition to being required for node protection, the autotunnel primary and backup feature provides the following benefits:
• Redundancy--If one backup tunnel is down, other backup tunnels protect LSPs.

• Increased backup capacity--If the protected interface is a high-capacity link and no single backup path exists with an equal capacity, multiple backup tunnels can protect that one high-capacity link. The LSPs using this link will fail over to different backup tunnels, allowing all of the LSPs to have adequate bandwidth protection during failure (rerouting). If bandwidth protection is not desired, the router spreads LSPs across all available backup tunnels (that is, there is load balancing across backup tunnels).

Scalability

A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

An example of N:1 protection is that when one backup tunnel protects 5000 LSPs, each router along the backup path maintains one additional tunnel.

An example of 1:1 protection is that when 5000 backup tunnels protect 5000 LSPs, each router along the backup path must maintain state for an additional 5000 tunnels.

RSVP Hello

RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, Hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

SSO Redundancy Overview

The SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

SSO is particularly useful at the network edge. It provides protection for network edge devices with dual route processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizes critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Affinity and Link Attributes with Autotunnel Backup

In Cisco IOS Release 15.1(1)S and later releases, you can use affinity and link attributes with the MPLS TE Autotunnel Backup feature to include or exclude links when configuring dynamic backup paths.
For a link, you can configure up to 32 bits of attribute flags, as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet0/0
Router(config-if)# mpls traffic-eng attribute-flags 0x22
```

The attribute flags are compared to the tunnel’s affinity bits during selection of the path.

When you enable the auto-tunnel backup feature, you can optionally specify the affinity and mask, as shown in the following example. If you do not specify an affinity and mask, the default for affinity is 0 and for the mask it is 0xFFFF is used. To ignore link affinity, use affinity and mask of 0. See the `mpls traffic-eng auto-tunnel backup config affinity` command for more information.

```
Router> enable
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x13 mask 0x13
```

The affinity/mask configured by the `mpls traffic-eng auto-tunnel backup config affinity` command is used for all dynamically created backup tunnels. The attribute mask determines which link attributes are relevant. If a bit in the mask is 0, the attribute is irrelevant. If a bit in the mask is 1, the attribute value of a link and the configured affinity of the tunnel for that bit must match.

In the figure below, there are two primary tunnels. One tunnel travels from router A to router B. The other primary tunnel travels from router A to router B and then router D. All the the links are configured with attribute flags 0x22. Both tunnels require fast reroute protection. To automatically create backup tunnels, enable the autotunnel backup feature with the `mpls traffic-eng auto-tunnel backup` command. However, the dynamically created backup tunnels do not come up, because attribute flags are configured on the links. To enable the dynamically created backup tunnels, you must also issue the following command:

```
Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22
```

![Figure 23: Specifying Link Attributes and Affinity with Autotunnel Backup](image)
# How to Configure MPLS Traffic Engineering Autotunnel Primary and Backup

## Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs

To establish an MPLS backup autotunnel to protect fast reroutable TE LSPs, perform the following task.

> **Note**
> Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `mpls traffic-eng auto-tunnel backup`
4. `mpls traffic-eng auto-tunnel backup nhop-only`
5. `mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]`
6. `mpls traffic-eng auto-tunnel backup timers removal unused sec`
7. `mpls traffic-eng auto-tunnel backup config unnumbered-interface interface`
8. `mpls traffic-eng auto-tunnel backup config affinity affinity-value mask mask-value`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> mpls traffic-eng auto-tunnel backup</td>
<td>Automatically builds NHOP and NNHOP backup tunnels.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# mpls traffic-eng auto-tunnel backup</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td><code>mpls traffic-eng auto-tunnel backup nhop-only</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# mpls traffic-eng auto-tunnel backup nhop-only</code></td>
</tr>
<tr>
<td>5</td>
<td><code>mpls traffic-eng auto-tunnel backup tunnel-num [min num] [max num]</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100</code></td>
</tr>
<tr>
<td>6</td>
<td><code>mpls traffic-eng auto-tunnel backup timers removal unused sec</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50</code></td>
</tr>
<tr>
<td>7</td>
<td><code>mpls traffic-eng auto-tunnel backup config unnumbered-interface interface</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0</code></td>
</tr>
<tr>
<td>8</td>
<td><code>mpls traffic-eng auto-tunnel backup config affinity affinity-value mask mask-value</code></td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22</code></td>
</tr>
</tbody>
</table>

**Establishing MPLS One-Hop Tunnels to All Neighbors**

To establish MPLS one-hop tunnels to all neighbors, perform the following task.

**Note**

Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.
### SUMMARY STEPS

1. enable
2. configure terminal
3. mpls traffic-eng auto-tunnel primary onehop
4. mpls traffic-eng auto-tunnel primary tunnel-num \([\text{min } num] [\text{max } num]\)
5. mpls traffic-eng auto-tunnel primary timers removal \(\text{rerouted } sec\)
6. mpls traffic-eng auto-tunnel primary config unnumbered \(\text{interface}\)
7. mpls traffic-eng auto-tunnel primary config mpls ip

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | **enable** | Enables privileged EXEC mode.  
- Enter your password if prompted. |
| Example: | Router> enable | |
| Step 2 | **configure terminal** | Enters global configuration mode. |
| Example: | Router# configure terminal | |
| Step 3 | **mpls traffic-eng auto-tunnel primary onehop** | Automatically creates primary tunnels to all next hops. |
| Example: | Router(config)# mpls traffic-eng auto-tunnel primary onehop | |
| Step 4 | **mpls traffic-eng auto-tunnel primary tunnel-num** \([\text{min } num] [\text{max } num]\) | Configures the range of tunnel interface numbers for primary autotunnels. |
| Example: | Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100 | |
| Step 5 | **mpls traffic-eng auto-tunnel primary timers removal** \(\text{rerouted } sec\) | Configures how many seconds after a failure primary autotunnels will be removed. |
| Example: | Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 400 | |
Exercise 1.1: Setting Up a Simple MPLS Label Switched Path (LSP)

**Objective:**
- Configure an MPLS LSP from a source to a destination router.

**Requirements:**
- Cisco IOS XE Software
- Source and destination routers

**Equipment Needed:**
- Two Cisco IOS XE routers
- Internet connectivity

**Procedure:**
1. **Install MPLS:**
   - Configure MPLS on both routers.
   ```conf
   Router(config)# router mpls
   ```
2. **Label Allocation:**
   - Assign labels to the LSP using LDP (Label Distribution Protocol).
   ```conf
   Router(config)# mpls traffic-eng ldp
   ```
3. **Path Protection:**
   - Enable path protection on LDP sessions.
   ```conf
   Router(config)# mpls traffic-eng ldp path-protection
   ```
4. **LSP Initiation:**
   - Create an LSP using LDP.
   ```conf
   Router(config)# mpls traffic-eng ldp session peer 10.0.0.1 local-label 100 remote-label 100
   ```
   - Using RSVP (Resource Reservation Protocol) to reserve resources for the LSP.
   ```conf
   Router(config)# mpls traffic-eng ldp session peer 10.0.0.1 local-label 100 remote-label 100
   ```

**Troubleshooting:**
- Check the LDP sessions using the `show ldp session` command.
- Verify MPLS LSPs using the `show mpls ldp lsp` command.

**Documentation:**
- Cisco IOS XE Configuration Guide
- MPLS Traffic Engineering Guidelines

---

**Example Configuration:**

```
Router(config)# mpls traffic-eng ldp
Router(config-lsp)# mpls traffic-eng ldp session peer 10.0.0.1 local-label 100 remote-label 100
Router(config)# mpls traffic-eng ldp path-protection
Router(config)# mpls traffic-eng ldp session peer 10.0.0.1 local-label 100 remote-label 100
```

---

**Note:**
This example shows the basic configuration for an LDP session and path protection. For a full LSP setup, additional configurations such as label distribution, path switching, and resource reservation are necessary.

---

**Conclusion:**
The exercise reinforces the understanding of MPLS configuration and the importance of label distribution and path protection in ensuring network reliability and efficiency.
POS2/2  10.0.0.45    YES  NVRAM  up    up
POS2/3  10.0.0.57    YES  NVRAM  administratively down  down
POS3/0  10.0.0.18    YES  NVRAM  down  down
POS3/1  10.0.0.33    YES  NVRAM  up    up
POS3/2  unassigned  YES  NVRAM  administratively down  down
POS3/3  unassigned  YES  NVRAM  administratively down  down
GigabitEthernet4/0  10.0.0.37    YES  NVRAM  up    up
GigabitEthernet4/1  unassigned  YES  NVRAM  administratively down  down
GigabitEthernet4/2  unassigned  YES  NVRAM  administratively down  down
Loopback0  10.0.3.1    YES  NVRAM  up    up
Tunnel0  10.0.3.1    YES  unset  up    up
Tunnel65436  10.0.3.1    YES  unset  up    up
Tunnel65437  10.0.3.1    YES  unset  up    up
Ethernet0  10.3.38.3    YES  NVRAM  up    up
Ethernet1  unassigned  YES  NVRAM  administratively down  down

R3-PRP#

The following command prevents autotunneling from creating NHOP backup tunnels:

Router# mpls traffic-eng auto-tunnel backup nhop-only

The "Type" field in the following show ip rsvp fast-reroute command shows that there is only an NHOP tunnel:

Router# show ip rsvp fast-reroute

Primary Protect BW Backup
Tunnel I/F BPS:Type Tunnel:Label State Level Type
-------- --------- ------------------------------- ------- ------- ------- -------
R3-PRP t0 POS/1 0:G Tu65436:24 Ready any-unl Nh

The following command changes the minimum and maximum tunnel interface numbers to 1000 and 1100, respectively:

Router# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100

You can verify the ID numbers and autotunnel backup range ID by entering the show ip rsvp fast-reroute and show ip interface brief commands. In this example, only one backup tunnel is protecting the primary tunnel:

Router# show ip rsvp fast-reroute

Primary Protect BW Backup
Tunnel I/F BPS:Type Tunnel:Label State Level Type
-------- --------- ------------------------------- ------- ------- ------- -------
R3-PRP t0 POS/1 0:G Tu1000:24 Ready any-unl Nh

Router# show ip interface brief

Interface I/F-Address OK? Method Status Protocol
POS2/0 10.0.0.14    YES  NVRAM  down  down
POS2/1 10.0.0.49    YES  NVRAM  up    up
POS2/2 10.0.0.45    YES  NVRAM  up    up
POS2/3 10.0.0.57    YES  NVRAM  administratively down  down
POS3/0 10.0.0.18    YES  NVRAM  down  down
POS3/1 10.0.0.33    YES  NVRAM  up    up
POS3/2 unassigned  YES  NVRAM  administratively down  down
POS3/3 unassigned  YES  NVRAM  administratively down  down
GigabitEthernet4/0 10.0.0.37    YES  NVRAM  up    up
GigabitEthernet4/1 unassigned  YES  NVRAM  administratively down  down
GigabitEthernet4/2 unassigned  YES  NVRAM  administratively down  down
Loopback0  10.0.3.1    YES  NVRAM  up    up
Tunnel0  10.0.3.1    YES  unset  up    up
Tunnel65436  10.0.3.1    YES  unset  up    up
Ethernet0  10.3.38.3    YES  NVRAM  up    up
Ethernet1 unassigned  YES  NVRAM  administratively down  down

The default tunnel range for autotunnel backup tunnels is 65,436 through 65,535. The following show ip rsvp fast-reroute command changes the tunnel range IDs:

Router# show ip rsvp fast-reroute
### Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs Example

<table>
<thead>
<tr>
<th>Primary</th>
<th>Protect</th>
<th>BW</th>
<th>Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel</td>
<td>I/F</td>
<td>BFS:Type</td>
<td>Tunnel:Label</td>
</tr>
<tr>
<td>--------</td>
<td>---------</td>
<td>-----------</td>
<td>--------------</td>
</tr>
<tr>
<td>R3-PRP_t0</td>
<td>PO3/1</td>
<td>0:G</td>
<td>Tu1001:0</td>
</tr>
</tbody>
</table>

The results are shown in the `show ip interface brief` command:

```bash
Router# show ip interface brief
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>UP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>POS2/0</td>
<td>10.0.0.14</td>
<td>YES</td>
<td>NVRAM</td>
<td>down</td>
<td>down</td>
</tr>
<tr>
<td>POS2/1</td>
<td>10.0.0.49</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>POS2/2</td>
<td>10.0.0.45</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>POS2/3</td>
<td>10.0.0.57</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>POS3/0</td>
<td>10.0.0.18</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>POS3/1</td>
<td>10.0.0.33</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>POS3/2</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM</td>
<td>administratively down</td>
<td>down</td>
</tr>
<tr>
<td>Loopback0</td>
<td>10.0.3.1</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel10</td>
<td>10.0.3.1</td>
<td>YES</td>
<td>unset</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel1000</td>
<td>10.0.3.1</td>
<td>YES</td>
<td>unset</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Tunnel1001</td>
<td>10.0.3.1</td>
<td>YES</td>
<td>unset</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet0</td>
<td>10.3.38.3</td>
<td>YES</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet1</td>
<td>unassigned</td>
<td>YES</td>
<td>NVRAM</td>
<td>administratively down</td>
<td>down</td>
</tr>
</tbody>
</table>

The following `mpls traffic-eng auto-tunnel backup timers removal unused` command specifies that a timer will scan backup autotunnels every 50 seconds and the timer will remove tunnels that are not being used:

```bash
Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50
```

The following `mpls traffic-eng auto-tunnel backup config unnumbered-interface` command enables IP processing on POS interface 3/1:

```bash
Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface POS3/1
```

To verify that IP processing is enabled on POS3/1, enter the `show interfaces tunnel` command:

```bash
Router# show interfaces tunnel 1001
```

The following `mpls traffic-eng auto-tunnel backup config affinity` command specifies affinity and link attributes that help in the calculation of the dynamically created backup tunnel:

```bash
Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22
```

To display the affinity and link attributes assigned to a dynamically created backup tunnel, enter the `show mpls traffic-eng auto-tunnel backup` command:

```bash
Router# show mpls traffic-eng auto-tunnel backup
```
Establishing MPLS One-Hop Tunnels to Neighbors Example

For autotunneling to automatically create primary tunnels to all next hops, you must enter the following command:

```
Router(config)# mpls traffic-eng auto-tunnel primary onehop
```

In this example there are four primary tunnels and no backup tunnels. To verify that configuration, enter the `show ip rsvp fast-reroute` command and the `show ip interface brief` command:

```
Router# show ip rsvp fast-reroute
Primary Protect BW Backup
Tunnel I/F BPS:Type Tunnel:Label State Level Type
-------- ------- -------------- ------ ------ ------- ----
R3-PRP_t65337 PO2/2 0:G None None None
R3-PRP_t65338 PO3/1 0:G None None None
R3-PRP_t65339 GI4/0 0:G None None None
R3-PRP_t65336 PO2/1 0:G None None None
```

```
Router# show ip interface brief
Interface IP-Address OK? Method Status Protocol
POS2/0 10.0.0.14 YES NVRAM down down
POS2/1 10.0.0.49 YES NVRAM up up
POS2/2 10.0.0.45 YES NVRAM up up
POS2/3 10.0.0.57 YES NVRAM administratively down down
POS3/0 10.0.0.18 YES NVRAM down down
POS3/1 10.0.0.33 YES NVRAM up up
POS3/2 unassigned YES NVRAM administratively down down
POS3/3 unassigned YES NVRAM administratively down down
GigabitEthernet4/0 10.0.0.37 YES NVRAM up up
GigabitEthernet4/1 unassigned YES NVRAM administratively down down
GigabitEthernet4/2 unassigned YES NVRAM administratively down down
Loopback0 10.0.3.1 YES NVRAM up up
Tunnel5337 10.0.3.1 YES unset administratively down down
Tunnel5336 10.0.3.1 YES unset up up
Tunnel5338 10.0.3.1 YES unset up up
Tunnel5339 10.0.3.1 YES unset up up
Ethernet0 10.3.38.3 YES NVRAM up up
Ethernet1 unassigned YES NVRAM administratively down down
R3-PRP#
```

The default tunnel range for primary autotunnels is 65,336 through 65,435. The following `mpls traffic-eng auto-tunnel primary tunnel-num` command changes the range to 2000 through 2100:

```
Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

The following sample output from the `show ip rsvp fast-reroute` command and the `show ip interface brief` command shows that the tunnel IDs are 2000, 2001, 2002, and 2003:

```
Router# show ip rsvp fast-reroute
Primary Protect BW Backup
Tunnel I/F BPS:Type Tunnel:Label State Level Type
-------- ------- -------------- ------ ------ ------- ----
R3-PRP_t2001 PO2/2 0:G None None None
R3-PRP_t2002 PO3/1 0:G None None None
R3-PRP_t2003 GI4/0 0:G None None None
```

MPLS Traffic Engineering Path, Link, and Node Protection Configuration Guide, Cisco IOS Release 15M&T
**Additional References**

The following sections provide references related to the MPLS Traffic Engineering-Autotunnel Primary and Backup feature.

**Related Topic** | **Document Title**
---|---
Backup tunnels | MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
Link protection | MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
MPLS traffic engineering commands | Cisco IOS Multiprotocol Label Switching Command Reference
SSO | Cisco IOS High Availability Configuration Guide
## Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

## MIBs

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

## RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

## Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></td>
</tr>
</tbody>
</table>
Feature Information for MPLS Traffic Engineering-Autotunnel Primary and Backup

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-Autotunnel Primary and Backup

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Traffic Engineering-Autotunnel Primary and Backup</td>
<td>12.0(27)S, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, 12.2(33)SRE, 15.1(1)S, Cisco IOS XE Release 2.3</td>
<td>The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels. In Cisco IOS Release 12.0(27)S, this feature was introduced. In Cisco IOS Release 12.2(33)SRA, this feature was integrated. In Cisco IOS Release 12.2(33)SXH, support was added. In Cisco IOS Release 12.4(20)T, this feature was integrated. In Cisco IOS Release 12.2(33)SRE, this feature was integrated. A router with primary one-hop autotunnels and backup autotunnels can be configured with SSO redundancy. In Cisco IOS Release 15.1(1)S, this feature was updated to allow you to specify affinity/mask for dynamically created MPLS TE backup tunnels. In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced: <code>affinity</code>, <code>mpls traffic-eng auto-tunnel backup config</code>, <code>show mpls traffic-eng auto-tunnel backup</code>.</td>
</tr>
</tbody>
</table>
Feature Name | Releases | Feature Configuration Information
---|---|---
MPLS TE - Autotunnel/Automesh SSO Coexistence | 15.2(1)T Cisco IOS XE Release 3.5S | In Cisco IOS XE Release 3.5S, this feature was integrated.
In Cisco IOS Release 15.2(1)T, 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 *MPLS High Availability Configuration Guide* for the new implementation.

---

**Glossary**

**backup tunnel** -- An MPLS traffic engineering tunnel used to protect other (primary) tunnel’s traffic when a link or node failure occurs.

**egress router** -- A router at the edge of the network where packets are leaving.

**Fast Reroute** -- Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**hop** -- Passage of a data packet between two network nodes (for example, between two routers).

**interface** -- A network connection.

**IP address** -- A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

**IP explicit path** -- A list of IP addresses, each representing a node or link in the explicit path.

**LDP** -- Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**link** -- Point-to-point connection between adjacent nodes.

**LSP** -- Label switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.
**LSR** -- label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

**MPLS** -- Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**node** -- Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

**penultimate router** -- The second-to-last router; that is, the router that is immediately before the egress router.

**primary tunnel** -- An MPLS tunnel whose LSP can be fast rerouted if there is a failure.

**router** -- A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**router ID** -- Something by which a router originating a packet can be uniquely distinguished from all other routers. For example, an IP address from one of the router's interfaces.

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

**traffic engineering** -- The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.
The MPLS Traffic Engineering: Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same Shared Risk Link Group (SRLG) as interfaces the backup tunnel is protecting.

SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

- Finding Feature Information, page 151
- Prerequisites for MPLS Traffic Engineering Shared Risk Link Groups, page 152
- Restrictions for MPLS Traffic Engineering Shared Risk Link Groups, page 152
- Information About MPLS Traffic Engineering Shared Risk Link Groups, page 152
- How to Configure MPLS Traffic Engineering Shared Risk Link Groups, page 157
- Configuration Examples for MPLS Traffic Engineering Shared Risk Link Groups, page 165
- Additional References, page 167
- Feature Information for MPLS Traffic Engineering Shared Risk Link Groups, page 169
- Glossary, page 172

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 Shared Risk Link Groups

• You must configure Fast Reroutable tunnels.
• You must enable the autotunnel backup.

Restrictions for MPLS Traffic Engineering Shared Risk Link Groups

• The backup tunnel must be within a single area.
• Manually created backup tunnels do not automatically avoid SRLGs of protected interfaces.
• A primary tunnel cannot be specified to avoid links belonging to specified SRLGs.

Information About MPLS Traffic Engineering Shared Risk Link Groups

MPLS Traffic Engineering Brief Overview

Multiprotocol Label Switching (MPLS) is an Internet Engineering Task Force (IETF)-specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

Traffic engineering (TE) is the process of adjusting bandwidth allocations to ensure that enough is left for high-priority traffic.

In MPLS TE, the upstream router creates a network tunnel for a particular traffic stream, then fixes the bandwidth available for that tunnel.

MPLS Traffic Engineering Shared Risk Link Groups

SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.

Backup tunnels should avoid using links in the same SRLG as interfaces they are protecting. Otherwise, when the protected link fails the backup tunnel fails too.

The figure below shows a primary label-switched path (LSP) from router R1 to router R5. The LSP protects against the failure of the R2-R3 link at R2 via a backup tunnel to R4. If the R2-R3 link fails, link protection
reroutes the LSP along the backup tunnel. However, the R2-R3 link and one of the backup tunnel links are in the same SRLG. So if the R2-R3 link fails, the backup tunnel may fail too.

**Figure 24: Backup Tunnel in the Same SRLG as the Interface It Is Protecting**

The MPLS TE SRLG feature enhances backup tunnel path selection so a backup tunnel can avoid using links that are in the same SRLG as the interfaces it is protecting.

There are two ways for a backup tunnel to avoid the SRLGs of its protected interface:

- The router does not create the backup tunnel unless it avoids SRLGs of the protected interface.
- The router *tries* to avoid SRLGs of the protected interface, but if that is not possible the router creates the backup tunnel anyway. In this case there are two explicit paths. The first explicit path *tries* to avoid the SRLGs of the protected interface. If that does not work, the backup tunnel uses the second path (which ignores SRLGs).

---

**Note**

Only backup tunnels that routers create automatically (called autotunnel backup) can avoid SRLGs of protected interfaces. For more information about these backup tunnels, see the [Autotunnel Backup for MPLS TE SRLGs](#), on page 155.

To activate the MPLS TE SRLG feature, you must do the following:

- Configure the SRLG membership of each link that has a shared risk with another link.
- Configure the routers to automatically create backup tunnels that avoid SRLGs of the protected interfaces.

For a detailed explanation of the configuration steps, see the [How to Configure MPLS Traffic Engineering Shared Risk Link Groups](#), on page 157.

Open Shortest Path First (OSPF) and Intermediate System-to-Intermediate System (IS-IS) flood the SRLG membership information (including other TE link attributes such as bandwidth availability and affinity) so that all routers in the network have the SRLG information for each link. With this topology information, routers can compute backup tunnel paths that exclude links having SRLGs in common with their protected...
interfaces. As shown in the figure below, the backup tunnel avoids the link between R2 and R3, which shares an SRLG with the protected interface.

**Figure 25: Backup Tunnel That Avoids SRLG of Protected Interface**

![Backup Tunnel](image)

### Fast Reroute Protection for MPLS TE SRLGs

Fast Reroute (FRR) protects MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on LSPs while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

Backup tunnels that bypass only a single link of the LSP’s path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP’s traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) backup tunnels because they terminate at the LSP’s next hop beyond the point of failure. The figure below illustrates an NHOP backup tunnel.

**Figure 26: NHOP Backup Tunnel**

![NHOP Backup Tunnel](image)

FRR provides node protection for LSPs. Backup tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop
node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic around the failed node to the next-next hop. FRR supports the use of Resource Reservation Protocol (RSVP) hellos to accelerate the detection of node failures. NNHOP backup tunnels also provide protection from link failures, because they bypass the failed link and the node.

The figure below illustrates an NNHOP backup tunnel.

*Figure 27: NNHOP Backup Tunnel*

---

**Autotunnel Backup for MPLS TE SRLGs**

Autotunnel backup is the ability of routers to create backup tunnels automatically. Therefore, you do not need to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface. Only automatically created backup tunnels can avoid SRLGs or their protected interfaces.

For information about backup tunnels, see the Fast Reroute Protection for MPLS TE SRLGs, on page 154. For detailed information about autotunnel backup and how you can change the default command values, see MPLS Traffic Engineering (TE)--AutoTunnel Primary and Backup.

To globally activate the autotunnel backup feature, enter the `mpls traffic-eng auto-tunnel backup` command.
The figure below illustrates an NNHOP automatically generated backup tunnel that excludes the router 192.168.1.1 and terminates at router R4. The backup tunnel must avoid touching any links of 192.168.1.1.

*Figure 28: Autotunnel Backup for NNHOP*

The figure below illustrates an NHOP automatically generated backup tunnel that terminates at router R3 and avoids the link 10.1.1.1, not the entire node.

*Figure 29: Autotunnel Backup for NHOP*

---

**Note**

NNHOP excludes the router ID (the entire router must be excluded; that is, no link of the router can be included in the backup tunnel’s path). NHOP excludes only the link when the backup tunnel’s path is computed.
How to Configure MPLS Traffic Engineering Shared Risk Link Groups

Configuring MPLS TE SRLG Membership of Each Link That Has a Shared Risk with Another Link

Perform the following task to configure MPLS TE SRLG membership of each link that has a shared risk with another link. Configuring SRLG membership enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same SRLG as interfaces the backup tunnel is protecting.

Enter the commands on the physical interface.

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. mpls traffic-eng srlg [number] [number]
5. mpls traffic-eng srlg end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>interface type slot/port</td>
<td>Specifies an interface and enters interface configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface pos 1/1/1</td>
<td>• The type argument is the type of interface to be configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The slot argument is the slot number. Refer to the appropriate hardware manual for slot and port information.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The /port argument is the port number. Refer to the appropriate hardware manual for slot and port information. The slash (/) is required.</td>
</tr>
</tbody>
</table>
### Configuring the Routers That Automatically Create Backup Tunnels to Avoid MPLS TE SRLGs

Perform the following task to configure routers that automatically create backup tunnels to avoid MPLS TE SRLGs of their protected interfaces. Backup tunnels provide link protection by rerouting traffic to the next hop bypassing failed links or in this instance by avoiding SRLGs.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `mpls traffic-eng auto-tunnel backup srlg exclude [force | preferred]`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
### Verifying the MPLS Traffic Engineering Shared Risk Link Groups Configuration

#### SUMMARY STEPS

1. `enable`
2. `show running-config`
3. `show mpls traffic-eng link-management interfaces interface slot/port`
4. `show mpls traffic-eng topology`
5. `show mpls traffic-eng topology srlg`
6. `show mpls traffic-eng topology brief`
7. `show mpls traffic-eng link-management advertisements`
8. `show ip rsvp fast-reroute`
9. `mpls traffic-eng auto-tunnel backup srlg exclude force`
10. `show ip explicit-paths`
11. `show mpls traffic-eng tunnels tunnel num`
12. `mpls traffic-eng auto-tunnel backup srlg exclude preferred`
13. `show ip explicit-paths`
14. `show ip rsvp fast-reroute`
15. `exit`

#### DETAILED STEPS

**Step 1** enable

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

```
Router# enable
Password: [Enter]
```

### Command or Action | Purpose
--- | ---
**Step 3** `mpls traffic-eng auto-tunnel backup srlg exclude [force | preferred]` | Specifies that autocreated backup tunnels should avoid SRLGs of its protected interface.

- The **force** keyword forces the backup tunnel to avoid SRLGs of its protected interface or interfaces.
- The **preferred** keyword causes the backup tunnel to try to avoid SRLGs of its protected interface or interfaces, but the backup tunnel can be created if SRLGs cannot be avoided.

**Example:**

```
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

### Step 4

**Example:**

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

**Purpose**

Returns to privileged EXEC mode.
Step 2  **show running-config**

Use the following commands to configure the SRLG membership of the interface pos 1/3/1 and to verify that the configuration is as expected. For example:

**Example:**

Router# configure terminal
Router(config)# interface pos 1/3/1
Router(config-if)# mpls traffic-eng srlg 1
Router(config-if)# mpls traffic-eng srlg 2
Router(config-if)# end
Router# show running-config

interface POS 1/3/1
ip address 10.0.0.33 255.255.255.255
no ip directed-broadcast
ip router isis
encapsulation ppp
no ip mroute-cache
mpls traffic-eng tunnels
mpls traffic-eng backup-path Tunnel5000
mpls traffic-eng srlg 1
mpls traffic-eng srlg 2
tag-switching ip
crc 32
clock source internal
pos ais-shut
pos report rdool
pos report lais
pos report lrdi
pos report pais
pos report prdi
pos report sd-ber
isis circuit-type level-2-only
ip rsvp bandwidth 20000 20000 sub-pool 5000

This verifies that the Packet over SONET (POS) interface pos 1/3/1 is associated that SRLG 1 and SRLG 2.

Step 3  **show mpls traffic-eng link-management interfaces interface slot/port**

Use this command to show the SRLG membership configured on interface pos 1/3/1. For example:

**Example:**

Router# show mpls traffic-eng link-management interfaces pos 1/3/1
System Information::
Links Count: 11
Link ID:: PO1/3/1 (10.0.0.33)
Link Status:
  SRLGs: 1 2
  Physical Bandwidth: 2488000 kbits/sec
  Max Res Global BW: 20000 kbits/sec (reserved:0% in, 0% out)
  Max Res Sub BW: 5000 kbits/sec (reserved:0% in, 0% out)
  MPLS TE Link State: MPLS TE on, RSVP on, admin-up, flooded
  Inbound Admission: allow-all
  Outbound Admission: allow-if-room
  Admin. Weight: 10 (IGP)
  IGP Neighbor Count: 1
  IGP Neighbor: 1D 0000.0000.0004.00, IP 10.0.0.34 (Up)
Flooding Status for each configured area [1]:
IGP Area[1]: isis level-2: flooded

**Step 4**  
**show mpls traffic-eng topology**

Use this command to show the SRLG link membership flooded via the Interior Gateway Protocol (IGP). For example:

**Example:**

```
Router# show mpls traffic-eng topology
```

```
My_System_id:0000.0000.0003.00 (isis level-2)
Signalling error holdown:10 sec Global Link Generation 9
IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node (isis level-2)
link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00, nbr_node_id:2, gen:9
   frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
   TE metric:10, IGP metric:10, attribute_flags:0x0
   SRLGs:1 2
   physical_bw:2488000 (kbps), max_reservable_bw_global:20000
   max_reservable_bw_sub:5000 (kbps)

<table>
<thead>
<tr>
<th>Total Allocated BW (kbps)</th>
<th>Global Pool</th>
<th>Reservable BW (kbps)</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>bw[0]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
<tr>
<td>bw[1]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
<tr>
<td>bw[2]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
<tr>
<td>bw[3]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
<tr>
<td>bw[4]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
<tr>
<td>bw[5]</td>
<td>0</td>
<td>20000</td>
<td>5000</td>
</tr>
</tbody>
</table>
```

**Step 5**  
**show mpls traffic-eng topology srlg**

Use this command to display all the links in the network that are members of a given SRLG. For example:

**Example:**

```
Router# show mpls traffic-eng topology srlg
```

```
MPLS TE Id:0000.0000.0003.00 (isis level-2)  
SRLG:1  
   10.0.0.33  
SRLG:2  
   10.0.0.33
```

The following command shows that there are two links in SRLG 1:

**Example:**

```
Router# show mpls traffic-eng topology srlg
```

```
MPLS TE Id:0000.0000.0003.00 (isis level-2)  
SRLG:1  
   10.0.0.33  
   10.0.0.49
```

**Step 6**  
**show mpls traffic-eng topology brief**

Use this command to display brief topology information:

**Example:**

```
Router# show mpls traffic-eng topology brief
```

```
My_System_id:0000.0000.0003.00 (isis level-2)
```
Step 7  show mpls traffic-eng link-management advertisements

Use this command to show local link information that MPLS TE link management is currently flooding into the global TE topology. For example:

Example:

Router# show mpls traffic-eng link-management advertisements

Flooding Status:  ready
Configured Areas:  1
IGP Area[1] ID::  isis level-2
System Information::
Flooding Protocol:  ISIS
Header Information::
  IGP System ID:  0000.0000.0003.00
  MPLS TE Router ID:  10.0.3.1
  Flooded Links:  2
Link ID::  0
  Link Subnet Type:  Point-to-Point
  Link IP Address:  10.0.0.49
  IGP Neighbor:  0000.0000.0007.00, IP 10.0.0.50
  TE metric:  80000
  IGP metric:  80000
  SRLGs:  None
  Physical Bandwidth:  622000 kbits/sec
  Res. Global BW:  20000 kbits/sec
  Res. Sub BW:  5000 kbits/sec
  Downstream::
  Global Pool  Sub Pool
  -----------  --------------
  Reservable Bandwidth[0]:  20000  5000 kbits/sec
  Reservable Bandwidth[1]:  20000  5000 kbits/sec
  Reservable Bandwidth[2]:  20000  5000 kbits/sec
  Reservable Bandwidth[3]:  20000  5000 kbits/sec
  Reservable Bandwidth[4]:  20000  5000 kbits/sec
  Reservable Bandwidth[5]:  20000  5000 kbits/sec
  Reservable Bandwidth[6]:  20000  5000 kbits/sec
  Reservable Bandwidth[7]:  20000  5000 kbits/sec
  Attribute Flags:  0x00000000
Link ID::  1
  Link Subnet Type:  Point-to-Point
  Link IP Address:  10.0.0.33
  IGP Neighbor:  0000.0000.0004.00, IP 10.0.0.34
  TE metric:  10
  IGP metric:  10
  SRLGs:  1
  Physical Bandwidth:  2488000 kbits/sec
  Res. Global BW:  20000 kbits/sec
  Res. Sub BW:  5000 kbits/sec
  Downstream::
  Global Pool  Sub Pool
  -----------  --------------
  Reservable Bandwidth[0]:  20000  5000 kbits/sec
  Reservable Bandwidth[1]:  20000  5000 kbits/sec
  Reservable Bandwidth[2]:  20000  5000 kbits/sec
  Reservable Bandwidth[3]:  20000  5000 kbits/sec
  Reservable Bandwidth[4]:  20000  5000 kbits/sec
  Reservable Bandwidth[5]:  20000  5000 kbits/sec
  Reservable Bandwidth[6]:  20000  5000 kbits/sec
  Reservable Bandwidth[7]:  20000  5000 kbits/sec

Verifying the MPLS Traffic Engineering Shared Risk Link Groups Configuration
Step 8  **show ip rsvp fast-reroute**

Use this command to show that the primary tunnel is going over Pos1/3/1 on R3, on which SRLG 1 is configured. For example:

**Example:**

```
Router# show ip rsvp fast-reroute
Primary  Protect  BW  Backup
Tunnel I/F  BPS:Type  Tunnel:Label  State  Level  Type
--------  -------  ------  --------  -----  -----  ----
R3-PRP_t0  PO1/3/1  0:G  None  None  None  None
```

Step 9  **mpls traffic-eng auto-tunnel backup srlg exclude force**

Use the following commands to configure autotunnel backup with the `force` keyword. For example:

**Example:**

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
Router(config)# exit
```

Step 10  **show ip explicit-paths**

Use the following command to verify that the `force` keyword is configured with the pos1/3/1 link excluded from the IP explicit path. For example:

**Example:**

```
Router# show ip explicit-paths
PATH __dynamic_tunnel65436 (loose source route, path complete, generation 24, status non-configured)
  1:exclude-address 10.0.0.33
  2:exclude-srlg  10.0.0.33
```

Step 11  **show mpls traffic-eng tunnels tunnel num**

Use the following command to show that autotunnel backup is configured but is down because the headend router does not have any other path to signal and it cannot use pos1/2/1 because it belongs in the same SRLG; that is, SRLG 1. For example:

**Example:**

```
Router# show mpls traffic-eng tunnels tunnel 65436
Name:R3-PRP_t65436 (Tunnel65436) Destination: 10.0.4.1
Status: Admin:up Oper:down Path:not valid Signalling:Down
path option 1, type explicit __dynamic_tunnel65436
Config Parameters:
  Bandwidth:0 kbps (Global) Priority:7 7 Affinity: 0x0/0xFFFF
  Metric Type:TE (default)
  AutoRoute: disabled LockDown:disabled Loadshare:0
bw-based
  auto-bw:disabled
  Shortest Unconstrained Path Info:
```
Step 12  **mpls traffic-eng auto-tunnel backup srlg exclude preferred**
The following commands configure autotunnel backup with the `preferred` keyword. For example:

**Example:**
```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude preferred
Router(config)# exit
```

Step 13  **show ip explicit-paths**
The following command shows two explicit paths. The first path avoids the SRLGs of the protected interface. The second path does not avoid the SRLGs. For example:

**Example:**
```
Router# show ip explicit-paths
PATH __dynamic_tunnel65436 (loose source route, path complete, generation 30, status non-configured)
  1:exclude-address 10.0.0.33
PATH __dynamic_tunnel65436_pathopt2 (loose source route, path complete, generation 33, status non-configured)
  1:exclude-address 10.0.0.33
```

Step 14  **show ip rsvp fast-reroute**
The following command shows that the primary tunnel is protected with autotunnel backup using the second path option (see Step 10) that does not avoid the SRLGs. For example:

**Example:**
```
Router# show ip rsvp fast-reroute
Primary Protect BW Backup
Tunnel I/F BPS:Type Tunnel:Label State Level Type
-------- ------- -------- ------------ ----- ----- ----
R3-PRP_t0 PO1/3/1 0:G 0:G Tu65436:0 Ready any-unl nhop
```

The following command shows the path options for the tunnel Tu65436:

**Example:**
```
Router# show mpls traffic-eng tunnels tunnel 65436
Name:R3-PRP_t65436 (Tunnel65436) Destination: 10.0.4.1
Status: Admin:up Oper:up Path:valid Signalling:connected
  path option 2, type explicit __dynamic_tunnel65436_pathopt2 (Basis for Setup, path weight 80020)
  path option 1, type explicit __dynamic_tunnel65436
Config Parameters:
  Bandwidth:0 kbps (Global) Priority:7 7 Affinity: 0x0/0xFFFF
```
Metric Type: TE (default)
AutoRoute: disabled  LockDown:disabled  Loadshare:0
bw-based
auto-bw:disabled
Active Path Option Parameters:
  State: explicit path option 2 is active
  Bandwidth Override: disabled  LockDown:disabled  Verbatim:disabled
InLabel : -
OutLabel : POS1/2/1, 23
RSVP Signalling Info:
  Src 10.0.3.1, Dst 10.0.4.1, Tun_Id 65436, Tun_Instance 3
  My Address: 10.0.3.1
  Explicit Route: 10.0.0.50 10.0.0.66 10.0.0.113 10.0.4.1
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 10 (TE)
  Explicit Route: 10.0.0.34 10.0.4.1

Step 15  exit
Use this command to exit to user EXEC mode. For example:

Example:

Router# exit
Router>

Configuration Examples for MPLS Traffic Engineering Shared Risk Link Groups

Configuring the SRLG Membership of Each Link That Has a Shared Risk with Another Link Example

The following example shows how to specify that the SRLG membership of each link has a shared risk with another link.

As shown in the figure below and in the following commands:

• link R2-R3 = SRLG5
• link R2-R3 = SRLG6
• link R7-R4 = SRLG5
• link R1-R2 = SRLG6
Configuring the Routers That Automatically Create Backup Tunnels to Avoid SRLGs Example

The following example shows how to specify that automatically created backup tunnels are forced to avoid SRLGs of their protected interfaces:

```
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup
Router(config)# mpls traffic-eng auto-tunnel backup srlg exclude force
```

The figure below illustrates the automatically created NNHOP backup tunnel that would be created to avoid SRLGs of the protected interface if the following conditions exist:

The exclude address is 192.168.1.1.

The link at R2 has an IP address of 10.1.1.1.
The backup tunnel’s explicit path avoids links that have a membership in the same SRLG as the link whose IP address is 10.1.1.1.

**Figure 31: srlg exclude force--NNHOP Autobackup Tunnel**

![NNHOP backup tunnel diagram]

The figure below illustrates the automatically created NHOP backup tunnel that would be created.

**Figure 32: srlg exclude force--NHOP Autobackup Tunnel**

![NHOP backup tunnel diagram]

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fast Reroute</td>
<td>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</td>
</tr>
<tr>
<td>Related Topic</td>
<td>Document Title</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Integrated IS-IS Routing Protocol Overview</td>
</tr>
<tr>
<td>OSPF</td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>Autotunnel backups</td>
<td>MPLS Traffic Engineering AutoTunnel Primary and Backup</td>
</tr>
</tbody>
</table>

### Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>--</td>
</tr>
</tbody>
</table>

### MIBs

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

### RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>draft-ietf-isis-gmpls-extensions-16.txt</td>
<td>IS-IS Extensions in Support of Generalized MPLS</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for MPLS Traffic Engineering Shared Risk Link 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 10: Feature Information for MPLS Traffic Engineering Shared Risk Link Groups

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Traffic Engineering: Shared Risk Link Groups</td>
<td>12.0(28)S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.0(29)S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SXH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.5S</td>
<td></td>
</tr>
<tr>
<td>Feature Name</td>
<td>Releases</td>
<td>Feature Information</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The MPLS Traffic Engineering: Shared Risk Link Groups feature enhances backup tunnel path selection so that a backup tunnel avoids using links that are in the same Shared Risk Link Group (SRLG) as interfaces the backup tunnel is protecting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may fail too. Links in the group have a shared risk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This document contains information about and instructions for configuring the MPLS Traffic Engineering Shared Risk Link Groups feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.0(28)S, this feature was introduced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.0(29)S, support was added for Open Shortest Path First (OSPF).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.2(33)SRA, this feature was integrated into a Cisco IOS 12.2SRA release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.2(33)SXH, this feature was integrated into a Cisco IOS 12.2SXH release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.4(20)T, this feature was integrated into a Cisco IOS 12.4T release.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS XE Release 3.5S, this feature was integrated into Cisco IOS XE Release 3.5S.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following commands were introduced or modified: mpls traffic-eng auto-tunnel backup srlg exclude, mpls traffic-eng srlg, show ip explicit-paths, show mpls traffic-eng link-management advertisements, show mpls</td>
</tr>
</tbody>
</table>
Glossary

**Fast Reroute** -- A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure. This protection allows data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

**hop** -- Passage of a data packet between two network nodes (for example, between two routers).

**IGP** -- Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system.

**interface** -- A network connection.

**IP address** -- A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

**IP explicit path** -- A list of IP addresses, each representing a node or link in the explicit path.

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

**LDP** -- Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

**link** -- A point-to-point connection between adjacent nodes.

**LSP** -- label-switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

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

**MPLS** -- Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**node** -- An endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

**OSPF** -- Open Shortest Path First. A link-state hierarchical Interior Gateway Protocol (IGP) routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.
**router** -- A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

**router ID** -- Something by which a router originating a packet can be uniquely distinguished from all other routers; for example, an IP address from one of the router's interfaces.

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

**tunnel** -- A secure communication path between two peers, such as two routers. A traffic engineering tunnel is a label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.
The MPLS Traffic Engineering: Inter-AS TE feature provides Autonomous System Boundary Router (ASBR) node protection, loose path reoptimization, stateful switchover (SSO) recovery of label-switched paths (LSPs) that include loose hops, ASBR forced link flooding, Cisco IOS Resource Reservation Protocol (RSVP) local policy extensions for interautonomous system (Inter-AS), and per-neighbor keys:

- **ASBR node protection**—Protects interarea and Inter-AS TE label-switched paths (LSPs) from the failure of an Area Border Router (ABR) or ASBR.
- **Loose path reoptimization**—Allows a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel’s LSPs to traverse hops that are not in the tunnel headend router’s topology database (that is, they are not in the same Open Shortest Path First (OSPF) area, Intermediate System-to-Intermediate System (IS-IS) level, or autonomous system as the tunnel’s headend router).
- **Loose hop recovery**—Supports SSO recovery of LSPs that include loose hops.
- **ASBR forced link flooding**—Helps an LSP cross a boundary into another domain when information in the other domain is not available to the headend router.
- **Cisco IOS RSVP local policy extensions for Inter-AS**—Allows network administrators to create controlled policies for TE tunnels that function across multiple autonomous systems.
- **Per-neighbor keys**—Allows cryptographic authentication to be accomplished on a per-neighbor basis.

- **Finding Feature Information**, page 176
- **Prerequisites for MPLS Traffic Engineering Inter-AS TE**, page 176
- **Restrictions for MPLS Traffic Engineering Inter-AS TE**, page 176
- **Information About MPLS Traffic Engineering Inter-AS TE**, page 177
- **How to Configure MPLS Traffic Engineering Inter-AS TE**, page 186
- **Configuration Examples for MPLS Traffic Engineering Inter-AS TE**, page 196
- **Additional References**, page 199
- **Feature Information for MPLS Traffic Engineering Inter-AS TE**, page 200
- **Glossary**, page 201
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 Inter-AS TE

- Enable MPLS.
- Configure TE on routers.
- Ensure that your network supports the following Cisco features:
  - MPLS
  - Cisco Express Forwarding
  - IS-IS or OSPF
- For loose path reoptimization, know how to configure the following:
  - IP explicit paths for MPLS TE tunnels
  - Loose hops
  - Interarea and Inter-AS tunnels

Restrictions for MPLS Traffic Engineering Inter-AS TE

Loose Path Reoptimization

- Midpoint reoptimization is not supported.

ASBR Forced Link Flooding

- The TE metric and affinity attributes that are known at a headend router (and used as constraints when an LSP’s path is computed) are not currently signaled. Consequently, explicit router (ERO) expansions do not consider these constraints.
- Each node in an autonomous system must have a unique router ID.
- The router ID configured on a link must not conflict with the router ID within the autonomous system.
- If a link is configured for forced link flooding, the link’s neighbors are not learned by regular Interior Gateway Protocol (IGP) updates. If a link is already learned about neighbors by IGP on a link, you
cannot configure the link as passive. Therefore, to configure a link for forced flooding, be sure that the node does not already have a neighbor on that link.

**Information About MPLS Traffic Engineering Inter-AS TE**

**MPLS Traffic Engineering Tunnels**

MPLS TE lets you build LSPs across your network that you then forward traffic down. MPLS TE LSPs, also called TE tunnels, let the headend of a TE tunnel control the path its traffic takes to a particular destination. This method is more flexible than forwarding traffic based only on a destination address. Interarea tunnels allow you to do the following:

- Build TE tunnels between areas (interarea tunnels)
- Build TE tunnels that start and end in the same area, on multiple areas on a router (intra-area tunnels)

Some tunnels are more important than others. For example, you may have tunnels carrying Voice over IP (VoIP) traffic and tunnels carrying data traffic that are competing for the same resources. Or you may simply have some data tunnels that are more important than others. MPLS TE allows you to have some tunnels preempt others. Each tunnel has a priority, and more-important tunnels take precedence over less-important tunnels.

**Multiarea Network Design**

You can establish MPLS TE tunnels that span multiple IGP areas and levels. The tunnel headend routers and tailend routers do not have to be in the same area. The IGP can be either IS-IS or OSPF.

To configure an interarea tunnel, use the `next-address loose` command to specify on the headend router a loosely routed explicit path of the LSP that identifies each ABR the LSP should traverse. The headend router and the ABRs along the specified explicit path expand the loose hops, each computing the path segment to the next ABR or tunnel destination.

**Fast Reroute**

MPLS Fast Reroute (FRR) is a fast recovery local protection technique that protects TE LSPs from link, shared risk link group (SRLG), and node failure. One or more TE LSPs (called backup LSPs) are preestablished to protect against the failure of a link, node, or SRLG. If there is a failure, each protected TE LSP traversing the failed resource is rerouted onto the appropriate backup tunnels.

The backup tunnel must meet the following requirements:

- It should not pass through the element it protects.
- It should intersect with a primary tunnel at a minimum of two nodes: point of local repair (PLR) and merge point (MP). The PLR should be the headend LSR of the backup tunnel, and the MP should be the tailend LSR of the backup tunnel. The PLR is where FRR is triggered when a link, node, or SRLG failure occurs.
• FRR protection can be performed for an Inter-AS tunnel only if the backup tunnel’s merge point can route packets to the PLR’s backup tunnel’s egress interface. You can configure a static route or you can configure Border Gateway Protocol (BGP) to export the backup tunnel’s egress interface to other autonomous systems.

• If the preferred link is a passive link, you must assign an administrative-weight for it. To assign an administrative weight, use the `mpls traffic-eng administrative-weight` command in interface configuration mode.

• Each router must be configured with the `mpls traffic-eng reoptimize events link-up` command in global configuration mode.

**ASBR Node Protection**

A TE LSP that traverses an ASBR needs a special protection mechanism (ASBR node protection) because the MP and PLR will be in different autonomous systems that have different IGPs.

A PLR ensures that the backup tunnel intersects with the primary tunnel at the MP by examining the Record Route Object (RRO) of the primary tunnel to see if any addresses specified in the RRO match the destination of the backup tunnel.

Addresses specified in RRO IPv4 and IPv6 subobjects can be node-IDs and interface addresses. The traffic engineering RFC 3209 specifies that you can use a router address or interface address, but recommends using the interface address of outgoing path messages. Therefore, in the figure below router R2 is more likely to specify interface addresses in the RRO objects carried in the resv messages of the primary tunnel (T1) and the backup tunnel.

Node IDs allow the PLR to select a suitable backup tunnel by comparing node IDs in the resv RRO to the backup tunnel’s destination.

RSVP messages that must be routed and forwarded to the appropriate peer (for example, an resv message) require a route from the MP back to the PLR for the RSVP messages to be delivered. The MP needs a route to the PLR backup tunnel’s outgoing interface for the resv message to be delivered. Therefore, you must configure a static route from the MP to the PLR. For the configuration procedure, see the Configuring a Static Route from the MP to the PLR, on page 188.
The figure below illustrates ASBR node protection. Router R4 is node-protected with a backup tunnel from R2-R3-R5-R6.

**Figure 33: ASBR Node Protection**

![Diagram showing ASBR node protection](image)

**Notes:**
- There are two autonomous systems.
- The numbers within the Ethernet serial connection indicate the OSPF area number.
- There is no IGP between R2 and R4, and R3 and R5.

In this configuration, IP addresses are as follows:

- **R1**--Loopback0 10.10.0.1
  - Ethernet 0--IP address of 10.10.1.1 is connected to R2 Ethernet 0
  - Ethernet 1--IP address of 10.10.2.1 is connected to R3 Ethernet 1

- **R2**--Loopback0 10.10.0.2
  - Ethernet 0--IP address of 10.10.1.2 is connected to R1 Ethernet 0
  - Ethernet 1--IP address of 10.10.3.1 is connected to R3 Ethernet 1
  - Serial 2--IP address of 10.10.4.1 is connected to R4 serial 2

- **R3**--Loopback0 10.10.0.3
  - Ethernet 0--IP address of 10.10.2.2 is connected to R1 Ethernet 1
  - Ethernet 1--IP address of 10.10.3.2 is connected to R2 Ethernet 1
Serial 2--IP address of 10.10.5.1 is connected to R5 serial 2

R4--Loopback0 10.10.0.4
  • Ethernet 0--IP address of 10.10.7.1 is connected to R6 Ethernet 0
  • Ethernet 1--IP address of 10.10.6.1 is connected to R5 Ethernet 1
  • Serial 2--IP address of 10.10.4.2 is connected to R2 serial 2

R5--Loopback0 10.10.0.5
  • Ethernet 0--IP address of 10.10.8.1 is connected to R6 Ethernet 0
  • Ethernet 1--IP address of 10.10.6.2 is connected to R4 Ethernet 1
  • Serial 2--IP address of 10.10.5.2 is connected to R3 serial 2

R6--Loopback0 10.10.0.6
  • Ethernet 0--IP address of 10.10.7.2 is connected to R4 Ethernet 0
  • Ethernet 1--IP address of 10.10.8.2 is connected to R5 Ethernet 1

In the figure above, the following situations exist:

• Routers R1, R2, and R3 are in AS 100. The R1-R2 and R1-R3 links are in OSPF area 1.
• Routers R4, R5, and R6 are in AS200. The R4-R6 and R5-R6 links are in OSPF area 2.
• The link R2-R3 is in AS100, and link R4-R5 is in AS200. The links R2-R3 and R4-R5 are in OSPF area 0.
• The links R2-R4 and R3-R5 are not running an IGP because they cross the Inter-AS boundary between AS100 and AS200. Because they are not running IGP, you must configure an administrative weight for each passive interface for FRR to work. Use the `mpls traffic-eng administrative-weight` command in interface configuration mode.
• There is a primary tunnel, tunnel 100, from R1-R2-R4-R6.
• There is a backup tunnel, tunnel 102, from R2-R3-R5-R6.
• There is a TE tunnel, tunnel 101, from R6-R5-R3-R1 for returning data traffic for tunnel 100.
• There is a TE tunnel, tunnel 103, from R6-R5-R3-R2 for returning data traffic for tunnel 102.
• The explicit paths of all the tunnels use loose hops.
• The R2-R4 link is configured to be link flooded in both R2’s and R4’s IGP. The R3-R5 link is configured to be link flooded in both R3’s and R5’s IGP.

Router R2 needs to ensure the following:

• Backup tunnel intersects with the primary tunnel at the MP, and therefore has a valid MP address. In the figure above, R2 needs to determine that tunnel 100 and backup tunnel 102 share MP node R6.
• Backup tunnel satisfies the request of the primary LSP for bandwidth protection. For example, the amount of bandwidth guaranteed for the primary tunnel during a failure, and the type of protection (preferably protecting against a node failure rather than a link failure).
Node-IDs Signaling in RROs

ASBR node protection includes a node-ID flag (0x20), which is also called a node-ID subobject. When it is set, the flag indicates that the address specified in the RRO object in the resv message is the node-ID address. The node-ID address refers to the traffic engineering router ID.

A node must always use the same address in the RRO (that is, it must use IPv4 or IPv6, but not both).

To display all the hops, enter the following command on the headend router. Sample command output is as follows:

```
Router(config)# show ip rsvp reservations detail
Reservation:
  Tun Dest: 10.10.0.6  Tun ID: 100  Ext Tun ID: 10.10.0.1
  Tun Sender: 10.10.0.1  LSP ID: 31
  Next Hop: 10.10.1.2 on Ethernet0/0
  Label: 17 (outgoing)
Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
Average Bitrate is 10K bits/sec, Maximum Burst is 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
RRO:
  10.10.0.2/32, Flags:0x29 (Local Prot Avail/to NNHOP, Is Node-id)
  10.10.4.1/32, Flags:0x9 (Local Prot Avail/to NNHOP)
    Label subobject: Flags 0x1, C-Type 1, Label 17
  10.10.0.4/32, Flags:0x20 (No Local Protection, Is Node-id)
    Label subobject: Flags 0x1, C-Type 1, Label 17
  10.10.7.1/32, Flags:0x0 (No Local Protection)
    Label subobject: Flags 0x1, C-Type 1, Label 0
  10.10.0.6/32, Flags:0x20 (No Local Protection, Is Node-id)
    Label subobject: Flags 0x1, C-Type 1, Label 0
Resv ID handle: 0100040E.
Status:
Policy: Accepted. Policy source(s): MPLS/TE
```

For a description of the fields, see the Cisco IOS Quality of Service Solutions Command Reference.

Addition of the Node-ID Subobject

When a fast reroutable LSP is signaled, the following actions occur:

- An LSR adds a node-ID subobject and an incoming label subobject in the resv message.
- If there is an RRO object in the path message, an LSR adds a node-ID subobject, an RRO IPv4 subobject that records the interface address, and an incoming label subobject in the resv message.

If you enable record-route on the headend LSR, the interface addresses for the LSP are included in the RRO object of the resv message.

To enable record-route, enter the following command with the `record-route` keyword:

```
tunnel mpls traffic-eng record-route
```

Processing of an RRO with Node-ID Subobjects

The node-ID subobject is added to the RECORD_ROUTE object before the label route subobject. If RECORD_ROUTE is turned on, the RRO object consists of the following in this order: node-ID, interface address, and label.

Merge Point Location

The destination of the backup tunnel is the node-ID of the MP. A PLR can find the MP and appropriate backup tunnel by comparing the destination address of the backup tunnel with the node-ID subobjects included in the resv RRO for the primary tunnel.
When both the IPv4 node-ID and IPv6 node-ID subobjects are present, a PLR can use either or both of them to find the MP address.

**Determination of Backward Compatibility**

To remain compatible with nodes that do not support RRO IPv4 or IPv6 node-ID subobjects, a node can ignore those objects. Those nodes cannot be the MP in a network with interarea or Inter-AS traffic engineering.

---

### Loose Path Reoptimization

#### Interarea and Inter-AS LSPs

If the LSP of an MPLS TE tunnel traverses hops that are not in the headend router’s topology database (that is, the hops are in a different OSPF area or IS-IS level), the LSP is called an interarea TE LSP.

If the LSP of the tunnel traverses hops that are in a different autonomous system (AS) from the tunnel’s headend router, the LSP is called an Inter-AS TE LSP.

Interarea LSPs and Inter-AS TE LSPs can be signaled using loose hop subobjects in their EROs. The headend does not have “strict” knowledge of hops beyond its area, so the LSP's path is "loosely" specified at the headend. Downstream routers processing these loose hop subobjects (which do have the knowledge) are relied upon to expand them into strict hops.

#### Loose Hop Configuration

Beyond the headend area, configure hops as loose hops. Typically you specify only the ABRs and the tailend router of a tunnel, but any other combination is allowed.

#### Loose Hop Expansion

Loose hop expansion is the conversion of a single ERO loose hop subobject into one or more strict hop subobjects.

Interarea and Inter-AS TE LSPs can be signaled using loose hop subobjects in their EROs. When a router receives a path message containing an ERO that has a loose hop as the next address, the router typically expands the ERO by converting the single loose hop subobject into one or more strict hop subobjects. The router typically has the knowledge, in its topology database, of the best way to reach the loose hop and computes this path by using constraint-based shortest path first (CSPF). So the router substitutes this more specific information for the loose hop subobject found in the ERO. This process is called loose hop expansion or ERO expansion.

Loose hop expansions can occur at one or more hops along an LSP’s path. This process is referred to as loose path reoptimization.

#### Tunnel Reoptimization Procedure

Tunnel reoptimization is the signaling of an LSP that is more optimal than the LSP a TE tunnel is currently using (for example, it may be shorter or may have a lower cost), and the switching over of the tunnel’s data to use this new LSP.

The new more optimal TE LSP is always established and the data moved onto it before the original LSP is torn down (so it is called the “make before break” procedure). This ensures that no data packets are lost during the transition to the new LSP.

For tunnel reoptimization to function:
• Each router must be configured with the `mpls traffic-eng reoptimize events link-up` command.

• Each passive link must have an assigned administrative weight. To configure an administrative weight, use the `mpls traffic-eng administrative-weight` command in interface configuration mode.

The TE LSPs reoptimization process is triggered under the following circumstances:

• Periodically (based on a timer)

• User entered a command (`mpls traffic-eng reoptimize`) requesting reoptimization

• Network event, such as a link-up

Regardless of how reoptimization is triggered, the headend router reoptimizes a tunnel only if it can find a better path than the one the tunnel currently uses. If there is not a better path in the local topology database, no new LSP is signaled and reoptimization does not occur.

Prior to the addition of loose path reoptimization, interarea TE LSPs were not reoptimized if a better path became available in any area beyond the headend area. This is because the headend router was not capable of finding a better path when the better path existed in an area beyond its view (that is, it was not in its local topology database).

With the addition of loose path reoptimization, a tunnel's headend can reoptimize LSPs even if they span multiple areas, levels, or autonomous systems. This is done via the implementation of a query and response protocol defined in `draft-vasseur-mpls-loose-path-reopt-02.txt`. This draft defines a protocol whereby a tunnel's headend may query downstream routers to perform ERO expansion for this tunnel's LSP. These downstream routers respond in the affirmative if they can find a more optimal path than the one in use. (This is done via a new ERO expansion.) Having received an affirmative answer to its query, a headend signals a new LSP for the tunnel, and the new LSP benefits from a new ERO expansion along the better path.

Loose path reoptimization is on by default, and cannot be disabled. Whenever an LSP reoptimization is attempted but the headend fails to find a better path, if the LSP contains loose ERO subobjects, a query is sent downstream to determine whether downstream routers can find a better path. If an affirmative answer comes back, the LSP is reoptimized. That is, a new LSP is signaled (which will follow the better path), the tunnel's data packets are switched over to use this new LSP, and the original LSP is torn down.

For details on this query and response protocol, see `draft-vasseur-mpls-loose-path-reopt-02.txt`.

### ASBR Forced Link Flooding

When you configure forced link flooding on an interface, the MPLS TE link management module advertises the link to all nodes. As a result of this advertisement, the TE topology database on all the nodes within the Inter-AS is updated with this information.

ASBR forced link flooding allows the links to be advertised even if IGP adjacencies are not running over these links. TE LSPs can traverse these links at the edge of a network between two nodes running BGP (or static routes) even if the exit ASBR is not listed in the IP explicit path. Therefore, a headend LSR can consider that link when it computes its TE LSP path.

### Configuration of ASBR Forced Link Flooding

To activate ASBR forced link flooding, configure a link as passive and provide neighbor information (that is, the neighbor IGP ID and the neighbor TE ID). The required configuration tasks are described in the `Configuring a Static Route from the MP to the PLR`, on page 188.
Link Flooding

A passive link is configured on an interface of an ASBR. The link is flooded in the ASBR’s IGP. All the links are flooded as point-to-point links. Flooding notifications are also sent when there is a change to a link’s property.

OSPF Flooding

OSPF floods opaque link-state advertisement (LSA) Type 10 link information. If a multiaccess link has more than one neighbor, a Type 10 LSA is advertised for each neighbor. In the topology database, neighbors are represented by point-to-point neighbor relationships.

Link TLV

A link TLV describes a single link and contains multiple sub-TLVs. An opaque LSA contains a single link TLV. For each ASBR-to-ASBR link, an ASBR must flood an opaque LSA containing one link TLV that has the link’s attributes.

A link TLV comprises the following sub-TLVs:

• Link type (1 octet)--(Required) Defines the type of the link. The link type of a passive interface always is 1 (point-to-point), even for a multiaccess subnetwork.

• Link ID (4 octets)--(Required) Identifies the other end of the link for a point-to-point link. Includes the system ID of the neighbor, requires static configuration for a multiaccess ASBR-to-ASBR link, and includes the system ID of the neighbor.

• Local interface IP address (4 octets)--(Required) Specifies the IP addresses of the neighbor’s interface corresponding to this link.

• Remote interface IP address (4 octets)--(Required) Specifies the IP addresses of the neighbor’s interface corresponding to this link. The remote interface IP address is set to the router ID of the next hop. There must be a static configuration for the ASBR-to-ASBR link.

• Traffic engineering metric (4 octets)

• Maximum bandwidth (4 octets)

• Maximum reservable bandwidth (4 octets)

• Unreserved bandwidth (32 octets)

• Administrative group (4 octets)

IS-IS TLV

In IS-IS, when autonomous system A1 floods its LSP, it includes the system ID and a pseudonode number. If three autonomous systems are connected to a multiaccess network LAN, each link is considered to be a point-to-point link. The links are marked with the maximum metric value so that the inter-ASBR links are considered by CSPF and not by shortest path first (SPF).

TE uses the protocol TLV type 22, which has the following data structure:

• System ID and pseudonode number node (7 octets)
• Default metric (3 octets)
• Length of sub-TLVs (1 octet)
• Sub-TLVs (0 to 244 octets), where each sub-TLV consists of a sequence of the following: 1 octet for subtype, 1 octet for the length of the value field of the sub-TLV, and 0 to 242 octets for the value

The table below defines the sub-TLVs.

### Table 11: Sub-TLVs

<table>
<thead>
<tr>
<th>Sub-TLV</th>
<th>Length (Octets)</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>4</td>
<td>Administrative group (color).</td>
</tr>
<tr>
<td>6</td>
<td>4</td>
<td>IPv4 address for the interface described by the main TLV.</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>IPv4 address for a neighboring router on this link. This will be set to the router ID of the next hop.</td>
</tr>
<tr>
<td>9</td>
<td>4</td>
<td>Maximum link bandwidth.</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>Reservable link bandwidth.</td>
</tr>
<tr>
<td>11</td>
<td>32</td>
<td>Unreserved bandwidth.</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>TE default metric.</td>
</tr>
<tr>
<td>250 to 254</td>
<td>--</td>
<td>Reserved for Cisco-specific extensions.</td>
</tr>
<tr>
<td>255</td>
<td>--</td>
<td>Reserved for future expansion.</td>
</tr>
</tbody>
</table>

The TE router ID is TLV type 134.

### Topology Database

When the topology database module receives a link-state advertisement (LSA), the module scans the LSA to find the neighbors of the links. The ASBR link is part of the same LSA and is installed in the TE topology database like any other link.

During the CSPF operation, the TE headend module uses the TE topology database to find a path to the destination. Because the Inter-AS links are part of the TE topology database, the CSPF operation uses these links to compute the LSP path.
Link Flooding

The IGP floods information about a link in the following situations:

- When a link goes down
- When a link’s configuration is changed (for example, when the link cost is modified)
- When it is time to periodically reflood the router’s IGP information
- When link bandwidth changes significantly

Flooding is a little different in IS-IS and OSPF. In OSPF, only information about the link that has changed is flooded, because a Type 10 LSA contains a single link advertisement. In IS-IS, information about all links on a node is flooded even if only one has changed, because the Type 22 TLV contains a list of all links on the router.

How to Configure MPLS Traffic Engineering Inter-AS TE

**Note**

There is no configuration procedure for loose path reoptimization.

Configuring Loose Hops

The section describes how to do the following so that there can be loose hops:

**Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link**

If you want a tunnel to span multiple networks, configure an explicit path on the tunnel that will cross the Inter-AS link by performing the following steps.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip explicit-path {name path-name | identifier number} [enable | disable]`
4. `next-address loose A.B.C.D`
5. `interface tunnel number`
6. `tunnel mpls traffic-eng fast-reroute`
7. `mpls traffic-eng reoptimize events link-up`
## DETAILED STEPS

| Step 1 | enable | Enables privileged EXEC mode.  
- Enter your password if prompted. |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Example:</strong></td>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>ip explicit-path {name path-name</td>
<td>identifier number} [enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# ip explicit-path identifier 2 enable</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>next-address loose A.B.C.D</td>
<td>Specifies the next loose IP address in the explicit path. Each area border router (ABR) the path must traverse should be specified in a <strong>next-address loose</strong> command. This command places the router in global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(cfg-ip-expl-path)# next-address loose 10.10.0.2</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td>interface tunnel number</td>
<td>Configures a tunnel interface. This command places the router in interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# interface tunnel 100</td>
<td></td>
</tr>
<tr>
<td>Step 6</td>
<td>tunnel mpls traffic-eng fast-reroute</td>
<td>Enables an MPLS traffic engineering tunnel to use an established backup tunnel in the event of a link failure.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config-if)# tunnel mpls traffic-eng fast-reroute</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td>mpls traffic-eng reoptimize events link-up</td>
<td>Enables automatic reoptimization of MPLS traffic engineering when an interface becomes operational.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# mpls traffic-eng reoptimize events link-up</td>
<td></td>
</tr>
</tbody>
</table>
Configuring a Route to Reach the Remote ASBR

SUMMARY STEPS

1. enable
2. configure terminal
3. ip route prefix mask {ip-address | interface-type interface-number}

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Step 3 ip route prefix mask {ip-address</td>
<td>interface-type interface-number}</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip route 10.10.0.1 255.255.255.255 tunnel 101</td>
<td></td>
</tr>
</tbody>
</table>

Configuring a Static Route from the MP to the PLR

To enable Fast Reroute protection that spans across different autonomous systems, configure a static route from the MP to the PLR by performing the following steps.

SUMMARY STEPS

1. enable
2. configure terminal
3. ip route prefix mask ip-address outgoing-interface
### Configuring ASBR Forced Link Flooding

This section describes how to do the following so that you can configure ASBR forced link flooding:

#### Configuring the Inter-AS Link as a Passive Interface Between Two ASBRs

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ip address ip-address mask [secondary]
5. mpls traffic-eng passive-interface nbr-te-id te-router-id [nbr-if-addr if-addr] [nbr-igp-id {isis sysid | ospf sysid}]
6. mpls traffic-eng administrative-weight weight

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
</tbody>
</table>

---

### Configuring ASBR Forced Link Flooding

This section describes how to do the following so that you can configure ASBR forced link flooding:

#### Configuring the Inter-AS Link as a Passive Interface Between Two ASBRs

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type slot/port
4. ip address ip-address mask [secondary]
5. mpls traffic-eng passive-interface nbr-te-id te-router-id [nbr-if-addr if-addr] [nbr-igp-id {isis sysid | ospf sysid}]
6. mpls traffic-eng administrative-weight weight

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Example:**
Router> enable | • Enter your password if prompted. |
| **Step 2**
**configure terminal** | Enters global configuration mode. |
| **Example:**
Router# configure terminal | |
| **Step 3**
**interface type slot/port** | Specifies an interface and enters interface configuration mode. Refer to the appropriate hardware manual for interface information. |
| **Example:**
Router(config)# interface serial 2/0 | |
| **Step 4**
**ip address ip-address mask [secondary]** | Sets a primary or secondary IP address for an interface. |
| **Example:**
Router(config-if)# ip address 10.10.4.1 255.255.255.0 | |
| **Step 5**
**mpls traffic-eng passive-interface nbr-te-id te-router-id [nbr-if-addr if-addr] [nbr-igp-id {isis sysid} | Configures a link as a passive interface between two ASBRs. |
| **Example:**
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.11.12 nbr-igp-id ospf 10.10.15.18 | For an RSVP Hello configuration on the Inter-AS link, all fields are required. |
| **Step 6**
**mpls traffic-eng administrative-weight weight** | Overrides the Interior Gateway Protocol (IGP) administrative weight (cost) of the link and assigns a specific weight for the link. |
| **Example:**
Router(config-if)# mpls traffic-eng administrative-weight 20 | |

**Creating LSPs Traversing the ASBRs**

To create LSPs traversing the ASBRs, perform the following steps.

**Note**

Perform Steps 3 through 7 for the primary LSP and then for the backup LSP.
SUMMARY STEPS

1. enable
2. configure terminal
3. ip explicit path name enable
4. next-address loose A.B.C.D
5. interface tunnel number
6. tunnel mpls traffic-eng fast-reroute
7. tunnel mpls traffic-eng path-option number {dynamic | explicit | {name path-name | path-number}} [lockdown]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip explicit path name enable</td>
<td>Specifies the name of the explicit path and enables the path.</td>
</tr>
<tr>
<td>Example: Router(config)# ip explicit path route1 enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> next-address loose A.B.C.D</td>
<td>Configures a loose hop.</td>
</tr>
<tr>
<td>Example: Router(config)# next-address loose 10.10.10.2</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> interface tunnel number</td>
<td>Configures a tunnel interface and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example: Router(config)# interface tunnel 100</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> tunnel mpls traffic-eng fast-reroute</td>
<td>Enables an MPLS traffic engineering tunnel to use an established backup tunnel in the event of a link failure.</td>
</tr>
<tr>
<td>Example: Router(config-if)# tunnel mpls traffic-eng fast-reroute</td>
<td></td>
</tr>
</tbody>
</table>
Configuring Multiple Neighbors on a Link

SUMMARY STEPS

1. enable
2. configure terminal
3. interface type slot/port
4. mpls traffic-eng passive-interface [nbr-te-id] [router-id | te-id] [nbr-igp-id] [isis sysid | ospf sysid]
5. mpls traffic-eng administrative-weight weight

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
</tbody>
</table>

| **Step 2** configure terminal | Enters global configuration mode. |
| **Example:** Router# configure terminal | |

| **Step 3** interface type slot/port | Specifies an interface and enters interface configuration mode. Refer to the appropriate hardware manual for interface information. |
| **Example:** Router(config)# interface serial 2/0 | |

| **Step 4** mpls traffic-eng passive-interface [nbr-te-id] [router-id | te-id] [nbr-igp-id] [isis sysid | ospf sysid] | Configures a link as a passive link. |
| **Example:** | |
### Command or Action

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command or Action</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overrides the Interior Gateway Protocol (IGP) administrative weight (cost) of the link and assigns a specific weight for the link.</td>
<td>mpls traffic-eng administrative-weight weight</td>
<td>Router(config-if)# mpls traffic-eng administrative-weight 20</td>
</tr>
</tbody>
</table>

#### Step 5

**Example:**

```
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
```

#### Troubleshooting Tips

The following debug commands are useful for troubleshooting issues with MPLS Traffic Engineering: Inter-AS TE.

**Debugging Headend of TE LSPs**

- debug mpls traffic-eng path lookup
- debug mpls traffic-eng path verify
- debug mpls traffic-eng path spf

**Debugging Head and Midpoint (Link-Related Debugs)**

- debug mpls traffic-eng link-management igp-neighbors
- debug mpls traffic-eng link-management advertisements
- debug mpls traffic-eng link-management bandwidth-allocation
- debug mpls traffic-eng link-management routing

### Verifying the Inter-AS TE Configuration

To verify the Inter-AS TE configuration, perform the following steps.

**Note**

Perform Step 1 for Fast Reroute ready, and Step 2 for Fast Reroute active.

**SUMMARY STEPS**

1. `show ip rsvp sender detail`
2. `show ip rsvp sender detail`
3. `show mpls traffic-eng link-management advertisements`
DETAILED STEPS

Step 1  show ip rsvp sender detail
Use this command to display the MP sender display for the primary tunnel when Fast Reroute is ready.

Example:

Router# show ip rsvp sender detail
PATH:
  Tunnel Dest: 10.10.0.6 Tunnel ID: 100 Ext Tunnel ID: 10.10.0.1
  Tunnel Sender: 10.10.0.1 LSP ID: 31
  Path refreshes:
    arriving: from PHOP 10.10.7.1 on Et0/0 every 30000 msecs
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: (0x7) Local Prot desired, Label Recording, SE Style
    Session Name: R1_t100
  ERO: (incoming)
    10.10.7.2 (Strict IPv4 Prefix, 8 bytes, /32)
    10.10.0.6 (Strict IPv4 Prefix, 8 bytes, /32)
  RRO:
    10.10.7.1/32, Flags:0x0 (No Local Protection)
    10.10.1.1/32, Flags:0x0 (No Local Protection)
    Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound FRR: Not active
    Outbound FRR: No backup tunnel selected
    Path ID handle: 50000416.
    Incoming policy: Accepted. Policy source(s): MPLS/TE
    Status: Proxy-terminated

Step 2  show ip rsvp sender detail
Use this command to display the MP sender display when the primary tunnel is Fast Reroute active:

Example:

Router# show ip rsvp sender detail
PATH:
  Tunnel Dest: 10.10.0.6 Tunnel ID: 100 Ext Tunnel ID: 10.10.0.1
  Tunnel Sender: 10.10.0.1 LSP ID: 31
  Path refreshes:
    arriving: from PHOP 10.10.3.1 on Et1/0 every 30000 msecs
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: (0x7) Local Prot desired, Label Recording, SE Style
    Session Name: R1_t100
  ERO: (incoming)
    10.10.0.4 (Strict IPv4 Prefix, 8 bytes, /32)
    10.10.0.6 (Loose IPv4 Prefix, 8 bytes, /32)
  RRO:
    10.10.3.1/32, Flags:0xB (Local Prot Avail/to NNHOP) !Ready
    10.10.1.1/32, Flags:0x0 (No Local Protection)
    Traffic params - Rate: 10K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound FRR: Active
    Orig Input I/F: Et0/0
    Orig PHOP: 10.10.7.1
    Now using Bkup Filterspec w/ sender: 10.10.3.1 LSP ID: 31
    Outbound FRR: No backup tunnel selected
    Path ID handle: 50000416.
Step 3  **show mpls traffic-eng link-management advertisements**

Use this command to display the influence of a passive link. On R2, the passive link to R4 is in the Link ID:: 1 section.

**Example:**

```
Router# show mpls traffic-eng link-management advertisements

Flooding Status: ready
Configured Areas: 2
IGP Area[1] ID:: ospf 1 area 0
System Information::
Flooding Protocol: OSPF
Header Information::
IGP System ID: 10.10.0.2
MPLS TE Router ID: 10.10.0.2
Flooded Links: 2
Link ID:: 1
Link Subnet Type: Point-to-Point
Link IP Address: 10.10.4.1
IGP Neighbor: ID 0-0-0-0-0-0-0, IP 10.10.0.4
Physical Bandwidth: 1544 kbits/sec
Res. Global BW: 1158 kbits/sec
Res. Sub BW: 0 kbits/sec
Downstream::

<table>
<thead>
<tr>
<th>Global Pool</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reservable Bandwidth[0]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[1]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[2]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[3]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[4]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[5]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[6]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[7]: 1148</td>
<td>0 kbits/sec</td>
</tr>
</tbody>
</table>

Attribute Flags: 0x00000000

IGP Area[1] ID:: ospf 1 area 1
System Information::
Flooding Protocol: OSPF
Header Information::
IGP System ID: 10.10.0.2
MPLS TE Router ID: 10.10.0.2
Flooded Links: 2
Link ID:: 1
Link Subnet Type: Point-to-Point
Link IP Address: 10.10.4.1
IGP Neighbor: ID 0-0-0-0-0-0-0, IP 10.10.0.4
Physical Bandwidth: 1544 kbits/sec
Res. Global BW: 1158 kbits/sec
Res. Sub BW: 0 kbits/sec
Downstream::

<table>
<thead>
<tr>
<th>Global Pool</th>
<th>Sub Pool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reservable Bandwidth[0]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[1]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[2]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[3]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[4]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[5]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[6]: 1158</td>
<td>0 kbits/sec</td>
</tr>
<tr>
<td>Reservable Bandwidth[7]: 1148</td>
<td>0 kbits/sec</td>
</tr>
</tbody>
</table>

Attribute Flags: 0x00000000
```

**Incoming policy:** Accepted. Policy source(s): MPLS/TE

**Status:** Proxy-terminated

**MPLS Traffic Engineering Path, Link, and Node Protection Configuration Guide, Cisco IOS Release 15M&T**

195
Configuration Examples for MPLS Traffic Engineering Inter-AS TE

Configuring Loose Hops Examples

Configuring an Explicit Path on the Tunnel That Will Cross the Inter-AS Link Example

The following commands configure a loose IP explicit path named route1 suitable for use as a path option with Inter-AS TE with the destination 10.10.10.6 that is to traverse ABRs 10.10.0.2 and 10.10.0.4. The tunnel headend and the specified ABRs will find a path from the source AS100 to the destination 10.10.0.6 in AS200. See the figure above.

Router(config)# ip explicit-path name route1 enable
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4
Router(cfg-ip-expl-path)# next-address loose 10.10.0.6

Note that the explicit path for an interarea TE tunnel need not specify the destination router because the tunnel configuration specifies it in the tunnel destination command. The following commands configure an explicit path named path-without-tailend that would work equally well for the interarea tunnel created in the previous example:

Router(config)# ip explicit-path name path-without-tailend
Router(cfg-ip-expl-path)# next-address loose 10.10.0.2
Router(cfg-ip-expl-path)# next-address loose 10.10.0.4

Configuring a Route to Reach the Remote ASBR in the IP Routing Table Example

In the following example, packets for the ASBR whose router ID is 10.10.0.1 will be forwarded via tunnel 101:

Router> enable
Router# configure terminal
Router(config)# ip route 10.10.0.1 255.255.255.255 tunnel 101

Configuring a Static Route from the MP to the PLR Example

In the following example, a static route is configured from the MP to the PLR. The outgoing interface is tunnel 103.

Router> enable
Router# configure terminal
Router(config)# ip route 10.10.3.1 255.255.255.255 tunnel 103
Configuring ASBR Forced Link Flooding Examples

Configuring the Inter-AS Link as a Passive Interface Example

For this example, see the figure above. Routers R2 and R4 have the following router IDs:

- Router R2--10.10.0.2
- Router R4--10.10.0.4

Router> enable
Router# configure terminal
Router(config)# interface serial 2/0

Configures OSPF on Router R2 When Its Neighbor Is Running OSPF Too

Router(config-if)# mpls traffic-end passive-interface nbr-te-id 10.10.0.4

Note
Because both routers are running OSPF, the nbr-igp-id keyword is not specified.

Specifies That Both Router R2 and Its Neighbor Are Running OSPF (the nbr-igp-id Keyword Is Specified)

Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4

Configures IS-IS on Router R1

Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id isis 40.0000.0002.0001.00

Configures the Neighbor IGP ID (nbr-igp-id) When There Is More than One Neighbor Specified on a Link

Router(config-if)# mpls traffic-end passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.7 nbr-igp-id ospf 10.10.0.7

Overrides the Interior Gateway Protocol (IGP) Administrative Weight of the Link and Assigns a Specific Weight

Router(config-if)# mpls traffic-eng administrative-weight 20

Note
The ID is unique for each neighbor.
Configures a Link as a Passive Interface (Includes Global TE Commands)

```
interface serial 2/0
ip address 10.10.4.1.255.255.255.0
mpls traffic-eng tunnels
mpls traffic-eng administrative-weight 10
mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
ip rsvp bandwidth 1000
mpls traffic-eng administrative-weight 20
```

Creating LSPs Traversing the ASBRs Example

In the following example, a primary LSP is created:

```
Router> enable
Router# configure terminal
Router(config)# ip explicit path route1 enable
Router(config)# next-address loose 10.10.0.2
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 100
Router(config-if)# tunnel mpls traffic-eng fast reroute
Router(config-if)# tunnel mpls traffic-eng path-option 1 route1
```

In the following example, a backup LSP is created:

```
Router> enable
Router# configure terminal
Router(config)# ip explicit path backpath1 enable
Router(config)# next-address loose 10.10.0.3
Router(config)# next-address loose 10.10.0.6
Router(config)# interface tunnel 102
Router(config)# mpls traffic-eng backup path tunnel 102
Router(config-if)# tunnel mpls traffic-eng path-option 1 backpath1
```

Configuring Multiple Neighbors on a Link Example

In the following example, there is more than one neighbor on a link:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/0
Router(config-if)# mpls traffic-eng passive-interface nbr-te-id 10.10.0.4 nbr-igp-id ospf 10.10.0.4
Router(config-if)# mpls traffic-eng administrative-weight 20
```
# Additional References

## Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS traffic engineering commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>Fast Reroute</td>
<td>MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)</td>
</tr>
<tr>
<td>Link flooding and node protection</td>
<td>MPLS Traffic Engineering: Interarea Tunnels</td>
</tr>
<tr>
<td>IS-IS configuration tasks</td>
<td>Configuring a Basic IS-IS Network</td>
</tr>
<tr>
<td>OSPF configuration tasks</td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>IS-IS and OSPF commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IP Routing Protocols Command Reference</td>
</tr>
<tr>
<td>RSVP</td>
<td>RSVP Message Authentication</td>
</tr>
</tbody>
</table>

## Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>--</td>
</tr>
</tbody>
</table>

## MIBs

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

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3209</td>
<td>Extensions to RSVP for LSP Tunnels</td>
</tr>
<tr>
<td>draft-ietf-mpls-rsvp-fastreroute-02.txt</td>
<td>Fast Reroute Extensions to RSVP-TE for LSP Tunnels</td>
</tr>
<tr>
<td>draft-vasseur-mpls-loose-path-reopt-02.txt</td>
<td>Reoptimization of an Explicitly Loosely Routed MPLS TE Path</td>
</tr>
<tr>
<td>draft-vasseur-mpls-inter-as-te-00.txt</td>
<td>MPLS Inter-AS Traffic Engineering</td>
</tr>
<tr>
<td>draft-ietf-mpls-soft-preemption-00.txt</td>
<td>MPLS Traffic Engineering Soft Preemption</td>
</tr>
</tbody>
</table>

### Technical Assistance

**Description**

The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.

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.

Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.

**Link**

[http://www.cisco.com/techsupport](http://www.cisco.com/techsupport)

### Feature Information for MPLS Traffic Engineering Inter-AS TE

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](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.
Table 12: Feature Information for MPLS Traffic Engineering: Inter-AS TE

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Traffic Engineering: Inter-AS TE</td>
<td>12.0(29)S</td>
<td>The MPLS Traffic Engineering: Inter-AS TE feature provides ASBR node protection, loose path reoptimization, SSO recovery of LSPs that include loose hops, ASBR forced link flooding, Cisco IOS RSVP local policy extensions for Inter-AS, and per-neighbor key capabilities. In 12.0(29)S, this feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRB</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.2(33)SXH</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.5S</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.0(29)S, this feature was introduced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.2(33)SRA, the <strong>nbr-if-addr</strong> keyword was added to the <strong>mpls traffic-eng passive-interface</strong> command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.2(33)SRB, support was added for SSO recovery of LSPs that include loose hops.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.2(33)SXH, this feature was integrated into Cisco IOS Release 12.2(33)SXH.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In 12.4(20)T, this feature was integrated into Cisco IOS Release 12.4(20)T.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS XE Release 3.5S, this feature was integrated into Cisco IOS XE Release 3.5S.</td>
</tr>
</tbody>
</table>

Glossary

**ABR** -- Area Border Router. A routers connecting two areas.

**adjacency** -- The MPLS TE Forwarding Adjacency feature allows a network administrator to handle a traffic engineering, label-switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm. A forwarding adjacency can be created between routers regardless of their location in the network. The routers can be located multiple hops from each other.

**area** -- A logical set of network segments (for example, one that is OSPF-based) and their attached devices. Areas usually are connected to other areas by routers, making up a single autonomous system. OSPF and IS-IS define their areas differently. OSPF area borders are marked by routers. Some interfaces are in one area, and other interfaces are in another area. With IS-IS, all the routers are completely within an area, and the area borders are on links, not on routers. The routers that connect the areas are level-2 routers, and routers that have no direct connectivity to another area are level-1 routers.
ASBR -- Autonomous System Boundary Router. The router is located between an OSPF autonomous system and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as RIP. ASBRs must reside in a nonstub OSPF area.

autonomous system -- A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas.

backup tunnel -- An MPLS traffic engineering tunnel used to protect other (primary) tunnel's traffic when a link or node failure occurs.

BGP -- Border Gateway Protocol. Interdomain routing protocol that replaces EGP. BGP exchanges reachability information with other BGP systems.

border router -- A router at the edge of a provider network that interfaces to another provider’s border router using extended BGP procedures.

Cisco Express Forwarding -- A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

Fast Reroute -- A mechanism for protecting MPLS traffic engineering (TE) LSPs from link and node failure by locally repairing the LSPs at the point of failure, allowing data to continue to flow on them while their headend routers attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

flooding -- A traffic-passing technique used by switches and bridges in which traffic received on an interface is sent out all the interfaces of that device except the interface on which the information was received originally.

forwarding adjacency -- A traffic engineering link (or LSP) into an IS-IS or OSPF network.

headend -- The router that originates and maintains a given LSP. This is the first router in the LSP’s path.

hop -- Passage of a data packet between two network nodes (for example, between two routers).

IGP -- Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Inter-AS LSP -- An MPLS traffic engineering label-switched path (LSP) that traverses hops that are not in the headend’s topology database (that is, it is not in the same OSPF area, IS-IS area, or autonomous system as the headend).

interface -- A network connection.

IP explicit path -- A list of IP addresses, each representing a node or link in the explicit path.

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

link -- A point-to-point connection between adjacent nodes.

LSA -- link-state advertisement. A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSAs are used by the receiving routers to maintain their routing tables.

LSP -- label-switched path. A configured connection between two routers, in which MPLS is used to carry packets. An LSP is a path created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.

midpoint -- A transit router for a given LSP.

midpoint reoptimization -- Ability of a midpoint to trigger a headend reoptimization.
MP --merge point. The LSR where one or more backup tunnels rejoin the path of the protected LSP, downstream of the potential failure. An LSR can be both an MP and a PLR simultaneously.

MPLS --Multiprotocol Label Switching. Packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

multicast --Single packets are copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination address field. (Multicast is an efficient paradigm for transmitting the same data to multiple receivers, because of its concept of a Group address. This allows a group of receivers to listen to the single address.)

node --Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be interconnected by links, and serve as control points in the network.

OSPF --Open Shortest Path First. A link-state, hierarchical Interior Gateway Protocol routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

opaque LSA --If a router understands LSA Type 10 link information, the router continues flooding the link throughout the network.

passive link --When IGP is not running on the link between two ASBRs, traffic engineering informs the IGP to flood link information on behalf of that link (that is, it advertises that link).

PLR --point of local repair. The headend LSR of a backup tunnel.

router --A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

RSVP --Resource Reservation Protocol. An IETF protocol used for signaling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.

SPF --shortest path first. A routing algorithm used as the basis for OSPF operations. When an SPF router is powered up, it initializes its routing-protocol data structures and then waits for indications from lower-layer protocols that its interfaces are functional.

SRLG --Shared Risk Link Group. Sets of links that are likely to go down together (for example, because they have the same underlying fiber).

tailend --The router upon which an LSP is terminated. This is the last router in the LSP's path.

TE --traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

TLV --type, length, values. A block of information embedded in Cisco Discovery Protocol advertisements.
CHAPTER 8

Configuring MPLS Traffic Engineering over GRE Tunnel Support

The MPLS Traffic Engineering (TE) over Generic Routing Encapsulation (GRE) Tunnel Support feature enables applications to establish TE tunnels over virtual interfaces.

- Finding Feature Information, page 205
- Prerequisites for Configuring MPLS TE over GRE Tunnel Support, page 205
- Restrictions for Configuring MPLS TE Over GRE Tunnel Support, page 206
- Information About Configuring MPLS TE over GRE Tunnel Support, page 206
- How to Configure MPLS TE over GRE Tunnel Support, page 207
- Configuration Examples for MPLS TE Over GRE Tunnel Support, page 213
- Additional References for MPLS TE Over GRE Tunnel Support, page 217
- Feature Information for MPLS TE Over GRE Tunnel Support, 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 Configuring MPLS TE over GRE Tunnel Support

Your network must support the following:

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

IPsec that is enabled on the GRE nodes to implement GRE traffic encryption

MPLS TE that is configured on the interface and on GRE tunnels

MPLS TE tunnels

If GRE tunnels and TE tunnels coexist within the same routing domain, routing loops will occur. Create separate routing domains by either configuring GRE overlay with static routing for GRE packets or using two separate routing processes, one for the GRE overlay and another for TE tunnels.

Restrictions for Configuring MPLS TE Over GRE Tunnel Support

The following TE features are not supported over GRE tunnels, so they should not be configured for TE tunnels that may traverse GRE tunnels:

- Autoroute destinations
- Automatic bandwidth adjustment
- Autotunnel primary one-hop tunnels
- Bidirectional Forwarding Detection (BFD)-triggered FRR
- Diff-Serve Aware TE (DS-TE)
- Explicit path options that identify excluded nodes
- Interarea/autonomous systems MPLS TE
- Point-to-multipoint TE
- Shared Risk Link Groups (SRLGs)
- Tunnel-Based Admission Control (TBAC)

GRE tunnels do not support Cisco nonstop forwarding with stateful switchover (NSF with SSO). If a switchover occurs, traffic loss occurs for TE over GRE, and the TE tunnels are resigaled.

Information About Configuring MPLS TE over GRE Tunnel Support

MPLS TE over GRE Tunnel Support Overview

MPLS TE tunnels provide transport for label switching data through an MPLS network using a path, which is constraint-based, and is not restricted to the IGP shortest cost path. The TE tunnels are usually established over physical links between adjacent routers. However, some applications require establishing TE tunnels over virtual interfaces such as GRE tunnels. Federal Information Processing Standard (FIPS) 140-2 compliance mandates that federal customers require traffic encryption throughout their network infrastructure, which is referred to as Type-I encryption level of security. Type-I encryption environments differentiate between
encrypted and unencrypted networks. The encrypted network is the secure part of the network that is in a secure facility, where encryption is not required. The unencrypted network is the unsecured part of the network where traffic encryption is required.

Two common methods of traffic encryption are as follows:

- External crypto devices
- Cisco IOS IPsec, which is the encryption embedded into Cisco IOS software

External crypto devices operate in Layer 2 (L2), providing link layer encryption of ATM and SONET traffic. Due to the migration of L2 networks to IP network, there is an increasing adoption of IP crypto devices and IPsec. This transition requires that the traffic encryption happens at the IP layer. The IP-based forwarding of service traffic, such as IP or Layer 3 (L3)/L2 VPN MPLS traffic, is implemented only through GRE tunnels.

**Benefits of MPLS TE over GRE Tunnel Support**

The MPLS TE Over GRE Tunnel Support feature enables you to leverage MPLS segmentation capabilities, such as Layer 2 and Layer 3 VPN, on GRE tunnel transport. This feature enables you to deploy MPLS TE to implement explicit path forwarding, FRR, and bandwidth management of traffic over GRE tunnels. Also, this feature helps maintain the TE capabilities currently supported by ATM legacy networks.

**How to Configure MPLS TE over GRE Tunnel Support**

**Configuring Resource Reservation Protocol Bandwidth**

**SUMMARY STEPS**

1. enable
2. configure terminal
3. interface type number
4. bandwidth kbps
5. ip address ip-address mask
6. mpls traffic-eng tunnels
7. tunnel source type number
8. tunnel destination \{host-name | ip-address | ipv6-address\}
9. ip rsvp bandwidth
10. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface type number</td>
<td>Configures a tunnel interface and enters interface configuration mode for the specified tunnel interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface tunnel 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>bandwidth kbps</td>
<td>Sets the total bandwidth for a bandwidth pool.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# bandwidth 100000</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>ip address ip-address mask</td>
<td>Configures a primary IP address for an interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip address 172.16.0.0 255.255.255.254</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>mpls traffic-eng tunnels</td>
<td>Enables traffic engineering tunnel signaling on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# mpls traffic-eng tunnels</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>tunnel source type number</td>
<td>Configures the source address for the tunnel interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# tunnel source loopback 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>tunnel destination {host-name</td>
<td>ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# tunnel destination 192.168.1.1</td>
<td>• ip-address—IP address of the host destination expressed in dotted decimal notation.</td>
</tr>
</tbody>
</table>
### Configuring an MPLS TE Tunnel

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `ip unnumbered type number`
5. `tunnel destination {host-name | ip-address | ipv6-address}`
6. `mpls traffic-eng tunnels`
7. `tunnel mpls traffic-eng priority setup-priority [hold-priority]`
8. `tunnel mpls traffic-eng bandwidth kbps`
9. `tunnel mpls traffic-eng path-option number dynamic`
10. `tunnel mpls traffic-eng fast-reroute`
11. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface tunnel number</td>
<td>Configures a tunnel interface and enters interface configuration mode for the specified tunnel interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface tunnel 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip unnumbered type number</td>
<td>Assigns an IP address to the tunnel interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ip unnumbered loopback 0</td>
<td>• An MPLS TE tunnel interface should be unnumbered because it represents a unidirectional link.</td>
</tr>
<tr>
<td><strong>Step 5</strong> tunnel destination {host-name</td>
<td>ip-address</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# tunnel destination 192.168.2.2</td>
<td>• ip-address—IP address of the host destination expressed in dotted decimal notation.</td>
</tr>
<tr>
<td><strong>Step 6</strong> mpls traffic-eng tunnels</td>
<td>Enables traffic engineering tunnel signaling on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# mpls traffic-eng tunnels</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> tunnel mpls traffic-eng priority setup-priority [hold-priority]</td>
<td>Configures the setup and reservation priority for the tunnel.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# tunnel mpls traffic-eng priority 7 7</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> tunnel mpls traffic-eng bandwidth kbps</td>
<td>Configures the bandwidth required for the tunnel.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# tunnel mpls traffic-eng bandwidth 10</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> tunnel mpls traffic-eng path-option number dynamic</td>
<td>Configures the path option for the tunnel.</td>
</tr>
</tbody>
</table>
### Configuring an MPLS TE Tunnel over GRE

#### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `interface tunnel number`
4. `ip unnumbered loopback number`
5. `tunnel destination ip-address`
6. `tunnel mpls traffic-eng autoroute announce`
7. `tunnel mpls traffic-eng`
8. `tunnel mpls traffic-eng path-option number dynamic`
9. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> tunnel mpls traffic-eng fast-reroute</td>
<td>Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# tunnel mpls traffic-eng fast-reroute</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> end</td>
<td>(Optional) Exits interface configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td><code>Router(config-if)# end</code></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>2</td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router# configure terminal</td>
</tr>
<tr>
<td>3</td>
<td>interface tunnel number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config)# interface tunnel 100</td>
</tr>
<tr>
<td>4</td>
<td>ip unnumbered loopback number</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# ip unnumbered loopback 0</td>
</tr>
<tr>
<td>5</td>
<td>tunnel destination ip-address</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# tunnel destination 10.255.1.2</td>
</tr>
<tr>
<td>6</td>
<td>tunnel mpls traffic-eng autoroute announce</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# tunnel mpls traffic-eng autoroute announce</td>
</tr>
<tr>
<td>7</td>
<td>tunnel mpls traffic-eng</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# tunnel mpls traffic-eng</td>
</tr>
<tr>
<td>8</td>
<td>tunnel mpls traffic-eng path-option number dynamic</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# tunnel mpls traffic-eng path-option 10 dynamic</td>
</tr>
<tr>
<td>9</td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-if)# end</td>
</tr>
</tbody>
</table>
Configuration Examples for MPLS TE Over GRE Tunnel Support

Example Configuring MPLS TE Over GRE Tunnel Support

The following example shows how to configure MPLS TE over a GRE tunnel between two routers: Router 1 and Router 2. The first loopback interface is used for router identification, and the other for reachability. One OSPF is used for TE and the other for reachability.

**Router 1**

```bash
configure terminal
no logging console
mpls traffic-eng tunnels
interface Loopback 0
   ip address 172.16.1.1 255.255.255.255
   no shutdown

interface Loopback 1
   ip address 10.255.1.1 255.255.255.0
   no shutdown

interface gigabitethernet 1/1
   ip address 172.16.1.1 255.255.255.255
   ip rsvp bandwidth 100000
   no shutdown

router ospf 172
   router-id 172.16.1.1
   network 172.16.0.0 0.0.255.255 area 0
   mpls traffic-eng router-id Loopback 0
   mpls traffic-eng area 0
   no shutdown

router ospf 10
   router-id 10.255.1.1
   network 10.255.0.0 0.0.255.255 area 0
   no shutdown

interface Tunnel 10
   bandwidth 20000
   ip address 172.16.0.1 255.255.255.252
   mpls traffic-eng tunnels
   keepalive 10 3
   tunnel source Loopback 1
   tunnel destination 10.255.1.2
   ip rsvp bandwidth 15000 sub-pool 5000

interface tunnel 100
   ip unnumbered loopback 0
   tunnel mode mpls traffic-eng
   tunnel destination 192.168.10.10
   tunnel mpls traffic-eng autoroute announce
   tunnel mpls traffic-eng path-option 10 dynamic

end
```

**Router 2**

```bash
configure terminal
no logging console
```
mpls traffic-eng tunnels
interface Loopback 0
ip address 172.16.1.2 255.255.255.255
no shutdown
!
interface Loopback 1
ip address 10.255.1.2 255.255.255.255
no shutdown
!
interface gigabitethernet 1/1
ip address 10.255.0.2 255.255.255.252
ip rsvp bandwidth 100000
no shutdown
!
routing ospf 172
router-id 172.16.1.2
network 172.16.0.0 0.0.255.255 area 0
mpls traffic-eng router-id Loopback 0
mpls traffic-eng area 0
no shutdown
!
routing ospf 10
router-id 10.255.1.2
network 10.255.0.0 0.0.255.255 area 0
no shutdown
!
interface Tunnel0
bandwidth 20000
ip address 172.16.0.2 255.255.255.252
mpls traffic-eng tunnels
keepalive 10 3
 Tunnel source Loopback 1
 Tunnel destination 10.255.1.1
ip rsvp bandwidth 15000 sub-pool 5000
!
interface Tunnel 100
ip unnumbered Loopback 0
tunnel mode mpls traffic-eng
tunnel destination 172.16.1.1
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 10 dynamic
!
e nd
Example Configuring CBTS with MPLS over GRE

The following example shows how to configure Class-Based Tunnel Selection (CBTS) with MPLS Traffic Engineering (TE) over GRE.

Figure 34: The Network Structure of CBTS with MPLS over GRE

Configuration of the Midpoint Router (R1)

```conf
mpls traffic-eng tunnels
!
interface Tunnel 102
ip address 203.20.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.0.1
tunnel key 22
tunnel checksum
ip rsvp bandwidth 500000
!
interface Tunnel 103
ip address 203.10.0.1 255.255.255.0
mpls ip
mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.10.1
tunnel key 33
tunnel checksum
ip rsvp bandwidth 500000
mpls traffic-eng tunnels
!router ospf 1
```
router-id 10.1.1.1
network 10.1.1.1 0.0.0.0 area 1
network 203.20.0.1 0.0.0.0 area 1
network 203.10.0.1 0.0.0.0 area 1
mpls traffic-eng router-id Loopback 0
mpls traffic-eng area 1

Configuration of the Head Router (R2)

mpls traffic-eng tunnels
!
interface Tunnel 203
 ip address 203.0.0.1 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.10.1
 tunnel key 6
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 211
 ip address 172.16.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
 tunnel source GigabitEthernet 0/0/0
 tunnel destination 192.168.20.1
 tunnel key 22
 tunnel checksum
 ip rsvp bandwidth 500000
!
interface Tunnel 2300
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
 tunnel mpls traffic-eng exp-bundle master
 tunnel mpls traffic-eng exp-bundle member Tunnel 2301
 tunnel mpls traffic-eng exp-bundle member Tunnel 2302
!
interface Tunnel 2301
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2301
 tunnel mpls traffic-eng exp 6 7
!
interface Tunnel 2302
 ip unnumbered Loopback 0
 tunnel mode mpls traffic-eng
 tunnel destination 10.3.3.3
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng autoroute metric relative -5
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 explicit name TE2302
 tunnel mpls traffic-eng exp default
!
router ospf 1
 router-id 10.2.2.2
 network 10.2.2.2 0.0.0.0 area 1
 network 203.20.0.2 0.0.0.0 area 1
 network 172.16.0.2 0.0.0.0 area 1
network 203.0.0.1 0.0.0.0 area 1
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 1
!  
ip explicit-path name TE2301 enable
next-address 203.0.0.2
ip explicit-path name TE2302 enable
next-address 172.16.0.1
next-address 172.26.0.2

Configuration of the Tail Router (R3)

mpls traffic-eng tunnels
!  
interface Tunnel 302
 ip address 203.0.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.0.1
tunnel key 6
tunnel checksum
ip rsvp bandwidth 500000
!  
interface Tunnel 311
 ip address 172.26.0.2 255.255.255.0
 mpls ip
 mpls traffic-eng tunnels
tunnel source GigabitEthernet 0/0/0
tunnel destination 192.168.20.1
tunnel key 33
tunnel checksum
ip rsvp bandwidth 500000
!
router ospf 1
 router-id 10.3.3.3
 network 10.3.3.3 0.0.0.0 area 1
 network 203.10.0.2 0.0.0.0 area 1
 network 172.26.0.2 0.0.0.0 area 1
 network 203.0.0.2 0.0.0.0 area 1
 mpls traffic-eng router-id Loopback0
 mpls traffic-eng area 1
!

Additional References for MPLS TE Over GRE Tunnel Support

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>MPLS commands</td>
<td>Cisco IOS Multiprotocol Label Switching Command Reference</td>
</tr>
</tbody>
</table>
Standards

<table>
<thead>
<tr>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-2</td>
<td>Security Requirements for Cryptographic Modules.</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS-TE-STD-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></td>
</tr>
</tbody>
</table>

RFCs

<table>
<thead>
<tr>
<th>RFC</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3812</td>
<td>MPLS TE Management Information Base (MIB)</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for MPLS TE Over GRE Tunnel 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 13: Feature Information for MPLS TE over GRE Tunnel Support

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS TE over GRE Tunnel Support</td>
<td>Cisco IOS XE Release 3.3S 15.2(1)T</td>
<td>The MPLS TE over GRE Tunnel Support feature enables applications to establish traffic engineering tunnels over virtual interfaces. The following commands were introduced or modified: <code>mpls traffic-eng tunnels</code>, <code>tunnel mpls traffic-eng autoroute announce</code>, <code>tunnel mpls traffic-eng bandwidth</code>, <code>tunnel mpls traffic-eng fast-reroute</code>, <code>tunnel mpls traffic-eng path-option</code>, <code>tunnel mpls traffic-eng priority</code>. In Cisco IOS XE 3.12S release, CBTS support was added for GRE interface type on the Cisco ASR 1000 Series Aggregation Services Routers.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.12S</td>
<td></td>
</tr>
</tbody>
</table>
MPLS Traffic Engineering—RSVP Graceful Restart

The MPLS Traffic Engineering—RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol (LDP) component) without losing its Multiprotocol Label Switching (MPLS) forwarding state. This feature has the following benefits:

- Graceful restart allows a node to recover state information from its neighbor when there is an RP failure or the device has undergone a stateful switchover (SSO).
- Graceful restart allows session information recovery with minimal disruption to the network.
- A node can perform a graceful restart to help a neighbor recover its state by keeping the label bindings and state information to provide a quick recovery of the failed node and not affect the traffic that is currently forwarded.

Finding Feature Information, page 221
Prerequisites for MPLS TE—RSVP Graceful Restart, page 222
Restrictions for MPLS TE—RSVP Graceful Restart, page 222
Information About MPLS TE—RSVP Graceful Restart, page 222
How to Configure MPLS TE—RSVP Graceful Restart, page 225
Configuration Examples for MPLS TE—RSVP Graceful Restart, page 229
Additional References, page 230
Feature Information for MPLS Traffic Engineering—RSVP Graceful Restart, page 231
Glossary, page 232

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—RSVP Graceful Restart

Perform the following tasks on routers before configuring the MPLS Traffic Engineering—RSVP Graceful Restart feature:

- Configure the Resource Reservation Protocol (RSVP).
- Enable MPLS.
- Configure traffic engineering (TE).
- Enable graceful restart.

Restrictions for MPLS TE—RSVP Graceful Restart

- Graceful restart supports node failure only.
- Cisco recommends that you configure interface hellos only if the neighbor router does not support node hellos.
- Unnumbered interfaces are not supported.
- You cannot configure an interface hello for graceful restart and an interface hello for Fast ReRoute or hello state timeout (HST) on the same interface.

Information About MPLS TE—RSVP Graceful Restart

Graceful Restart Operation

RSVP graceful restart allows RSVP TE enabled nodes to recover gracefully following a node failure in the network such that the RSVP state after the failure is restored as quickly as possible. The node failure may be completely transparent to other nodes in the network.

RSVP graceful restart preserves the label values and forwarding information and works with third-party or Cisco routers seamlessly.

RSVP graceful restart depends on RSVP hello messages to detect that a neighbor went down. Hello messages include Hello Request or Hello Acknowledgment (ACK) objects between two neighbors.

A node hello is transmitted when graceful restart is globally configured and the first LSP to the neighbor is created.

Interface hello is an optional configuration. If you configure the graceful restart Hello command on an interface, the interface hello is considered to be an additional hello instance with the neighbor.
The router transmits an interface hello for graceful restart when all of the following conditions are met:

- Graceful restart is configured globally.
- Graceful restart is configured on the interface.
- An LSP to the neighboring router is created and goes over the interface.

Cisco recommends that you use node hellos if the neighbor supports node hellos, and configure interface hellos only if the neighbor router does not support node hellos.

Interface hellos differ from node hellos as follows:

- **Interface hello** — The source address in the IP header of the hello message has an IP address that matches the interface that the Hello message sent out. The destination address in the IP header is the interface address of the neighbor on the other side of the link. A TTL of 1 is used for per-interface hellos as it is destined for the directly-connected neighbor.

- **Node hello** — The source address in the IP header of the Hello message includes the TE router ID of the sending router. The destination address of the IP header has the router ID of the neighbor to which this message is sent. A TTL of more than 1 is used.

The figure below shows the graceful restart extension to these messages that an object called Restart_Cap, which tells neighbors that a node, may be capable of restarting if a failure occurs. The time-to-live (TTL) in these messages is set to 255 so that adjacencies can be maintained through alternate paths even if the link between two neighbors goes down.

*Figure 35: How Graceful Restart Works*

The Restart_Cap object has two values—the restart time, which is the sender’s time to restart the RSVP_TE component and exchange hello messages after a failure; and the recovery time, which is the desired time that the sender wants the receiver to synchronize the RSVP and MPLS databases.

In the figure above, graceful restart is enabled on Router 1, Router 2, Router 3, and Router 4. For simplicity, assume that all routers are restart capable. A TE label switched path (LSP) is signaled from Router 1 to Router 4.

Router 2 and Router 3 exchange periodic graceful restart hello messages every 10000 ms (10 seconds), and so do Router 2 and Router 1 and Router 3 and Router 4. Assume that Router 2 advertises its restart time as 60000 ms (60 seconds) and its recovery time as 60000 ms (60 seconds) as shown in the following example:

```
23:33:36: Outgoing Hello:
23:33:36: HELLO type HELLO REQUEST length 12:
23:33:36: Src_Instance: 0x6EDA8BD7, Dst_Instance: 0x00000000
```
23:33:36:  RESTART_CAP type 1 length 12:
23:33:36:  Restart_Time: 0x0000EA60
       , Recovery_Time: 0x0000EA60

**Note**
The restart and recovery time are shown in **bold** in the last entry.

Router 3 records this into its database. Also, both neighbors maintain the neighbor status as UP. However, Router 3’s control plane fails at some point (for example, a Primary Route Processor failure). As a result, RSVP and TE lose their signaling information and states although data packets continue to be forwarded by the line cards.

When four ACK messages are missed from Router 2 (40 seconds), Router 3 declares communication with Router 2 lost “indicated by LOST” and starts the restart time to wait for the duration advertised in Router 2’s restart time previously and recorded (60 seconds). Router 1 and Router 2 suppress all RSVP messages to Router 3 except hellos. Router 3 keeps sending the RSVP Path and Resv refresh messages to Router 4 and Router 5 so that they do not expire the state for the LSP; however, Router 3 suppresses these messages for Router 2.

**Note**
A node restarts if it misses four ACKs or its hello src_instance (last source instance sent to its neighbor) changes so that its restart time = 0.

Before the restart time expires, Router 2 restarts and loads its configuration and graceful restart makes the configuration of Router 2 send the hello messages with a new source instance to all the data links attached. However, because Router 2 has lost the neighbor states, it does not know what destination instance it should use in those messages; therefore, all destination instances are set to 0.

When Router 3 sees the hello from Router 2, Router 3 stops the restart time for Router 2 and sends an ACK message back. When Router 3 sees a new source instance value in Router 2’s hello message, Router 3 knows that Router 2 had a control plane failure. Router 2 gets Router 3’s source instance value and uses it as the destination instance going forward.

Router 3 also checks the recovery time value in the hello message from Router 2. If the recovery time is 0, Router 3 knows that Router 2 was not able to preserve its forwarding information and Router 3 deletes all RSVP state that it had with Router 2.

If the recovery time is greater than 0, Router 1 sends Router 2 Path messages for each LSP that it had previously sent through Router 2. If these messages were previously refreshed in summary messages, they are sent individually during the recovery time. Each of these Path messages includes a Recovery_Label object containing the label value received from Router 2 before the failure.

When Router 3 receives a Path message from Router 2, Router 3 sends a Resv message upstream. However, Router 3 suppresses the Resv message until it receives a Path message.
# How to Configure MPLS TE—RSVP Graceful Restart

## Enabling Graceful Restart

Note: It is optional that you configure graceful restart on an interface.

### SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `ip rsvp signalling hello graceful-restart mode help-neighbor`
4. `interface type number`
5. `ip rsvp signalling hello graceful-restart`
6. `exit`

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip rsvp signalling hello graceful-restart mode help-neighbor</td>
<td>Sets the number of DSCP hello messages on a neighboring router with restart capability.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> interface type number</td>
<td>(Optional) Configures the interface type and number and enters interface configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface POS 1/0/0</td>
<td></td>
</tr>
</tbody>
</table>
Setting a DSCP Value

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip rsvp signalling hello graceful-restart dscp num
4. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip rsvp signalling hello graceful-restart dscp num</td>
<td>Sets the number of DSCP hello messages on a graceful restart-enabled router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# ip rsvp signalling hello graceful-restart dscp 30</td>
<td></td>
</tr>
</tbody>
</table>
### Setting a Hello Refresh Interval

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip rsvp signalling hello graceful-restart refresh interval interval-value`
4. `end`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>ip rsvp signalling hello graceful-restart refresh interval interval-value</code></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000</code></td>
</tr>
<tr>
<td></td>
<td>Sets a hello refresh interval on a router with graceful restart enabled.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router(config)# end</code></td>
</tr>
<tr>
<td></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
# Setting a Missed Refresh Limit

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello graceful-restart refresh misses** <i>msg-count</i>
4. **end**

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>ip rsvp signalling hello graceful-restart refresh misses</strong> &lt;i&gt;msg-count&lt;/i&gt;</td>
<td>Sets a refresh limit on a router with graceful restart enabled.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>end</strong></td>
<td>Exits to privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>
Verifying Graceful Restart Configuration

SUMMARY STEPS

1. enable
2. show ip rsvp hello graceful-restart
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Enable</td>
<td>- Enter your password if prompted.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Displays information about the status of graceful restart and related parameters.</td>
</tr>
<tr>
<td>show ip rsvp hello graceful-restart</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show ip rsvp hello graceful-restart</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Exits to user EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td>Example:</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# end</td>
</tr>
</tbody>
</table>

Configuration Examples for MPLS TE—RSVP Graceful Restart

MPLS TE—RSVP Graceful Restart Example

In the following example, graceful restart is enabled, and related parameters, including a DSCP value, a refresh interval, and a missed refresh limit are set:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 10000
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 4
Router(config)# end
```
The following example verifies the status of graceful restart and the configured parameters:

```
Router# show ip rsvp hello graceful-restart
Graceful Restart:Enabled (help-neighbor only)
 Refresh interval:10000 msecs
 Refresh misses:4
 DSCP:0x30
 Advertised restart time:0 secs
 Advertised recovery time:0 secs
 Maximum wait for recovery:3600000 secs
```

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples</td>
<td>Cisco IOS Quality of Service Solutions Command Reference</td>
</tr>
<tr>
<td>Quality of service (QoS) classification</td>
<td>Classification Overview</td>
</tr>
<tr>
<td>QoS signalling</td>
<td>Signalling Overview</td>
</tr>
<tr>
<td>QoS congestion management</td>
<td>Congestion Management Overview</td>
</tr>
<tr>
<td>Stateful switchover</td>
<td>Stateful Switchover</td>
</tr>
<tr>
<td>MPLS Label Distribution Protocol</td>
<td>MPLS Label Distribution Protocol (LDP)</td>
</tr>
<tr>
<td>Information on stateful switchover, Cisco nonstop forwarding, graceful restart</td>
<td>NSF/SSO—MPLS TE and RSVP Graceful Restart</td>
</tr>
<tr>
<td>RSVP hello state timer</td>
<td>MPLS Traffic Engineering: RSVP Hello State Timer</td>
</tr>
</tbody>
</table>

#### Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.</td>
<td>—</td>
</tr>
</tbody>
</table>
MIBs

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

RFCs

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC 3209</td>
<td>RSVP-TE: Extensions to RSVP for LSP Tunnels</td>
</tr>
<tr>
<td>RFC 3478</td>
<td>Graceful Restart Mechanism for Label Distribution</td>
</tr>
</tbody>
</table>

Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for MPLS Traffic Engineering—RSVP Graceful Restart

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 14: Feature Information for MPLS Traffic Engineering—RSVP Graceful Restart

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS Traffic Engineering—RSVP Graceful Restart</td>
<td>12.0(29)S</td>
<td>The MPLS TE—RSVP Graceful Restart feature allows a neighboring Route Processor (RP) to recover from disruption in control plane service (specifically, the Label Distribution Protocol (LDP) component) without losing its MPLS forwarding state.</td>
</tr>
<tr>
<td></td>
<td>12.2(33)SRE</td>
<td>In Cisco IOS Release 12.0(29)S, this feature was introduced.</td>
</tr>
<tr>
<td></td>
<td>12.4(20)T</td>
<td>In Cisco IOS Release 12.4(20)T, this feature was integrated.</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 2.3</td>
<td>The following commands were introduced or modified:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ip rsvp signalling hello graceful-restart dscp, ip rsvp signalling hello graceful-restart mode help-neighbor, ip rsvp signalling hello graceful-restart refresh interval, ip rsvp signalling hello graceful-restart refresh misses, show ip rsvp counters, show ip rsvp counters state teardown, show ip rsvp hello, show ip rsvp hello client lsp detail, show ip rsvp hello client lsp summary, show ip rsvp hello client neighbor detail, show ip rsvp hello client neighbor summary, show ip rsvp hello graceful-restart, show ip rsvp hello instance detail, show ip rsvp hello instance summary.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Cisco IOS Release 12.2(33)SRE, per node hellos allow interoperability with Cisco IOS Release 12.0S.</td>
</tr>
</tbody>
</table>

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) tunnels’ 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.

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. A configured connection between two routers, in which MPLS is used to carry packets. A path created by the concatenation of one or more label switched hops, allowing a packet to be forwarded by swapping labels from an MPLS node to another MPLS node.

merge point—The tail of the backup tunnel.

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.

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.

RP—Route processor. Processor module in routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor.

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.