MPLS Traffic Engineering (TE) Path Protection

Last Updated: November 29, 2011

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

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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).

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

- 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 FRR flag.
- Dynamic diverse paths are not supported.
- Do not use link and node protection with path protection on the headend router.
- Do not configure path protection on an automesh tunnel template because the destinations are different and you cannot use the same path option to reach multiple destinations.

Information About MPLS Traffic Engineering (TE) Path Protection

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.

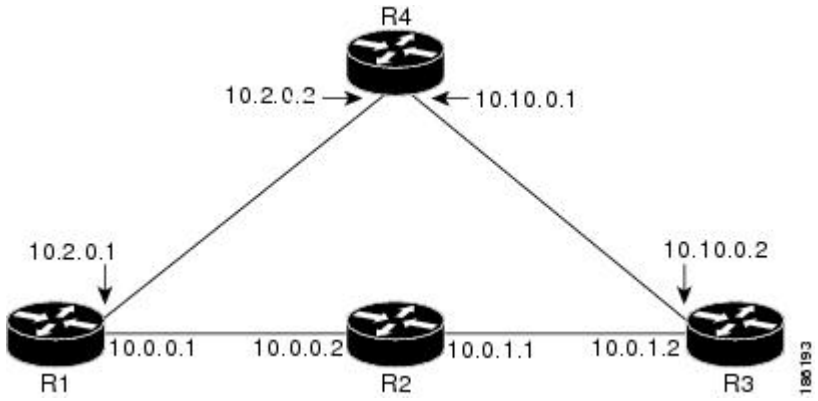
If the primary LSP was active during the switchover, only the primary LSP is recovered. The secondary LSP that was signaled and that provided path protection is resignaled after the TE recovery period is complete. This does not impact traffic on the tunnel because the secondary LSP was not carrying traffic.

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 1 Network Topology--Path Protection



Configuring Explicit Paths for Secondary Paths

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip explicit-path** {**name** *path-name*| **identifier** *number*} [**enable**	**disable**] **Example:** `Router(config)# ip explicit-path name path3441 enable`	Creates or modifies the explicit path and enters IP explicit path command mode.
Step 4	**index** *index command ip-address* **Example:** `Router(cfg-ip-exp1-path)# index 1 next-address 10.0.0.1`	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.

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(cfg-ip-exp1-path)# exit`	Exits IP explicit path command mode and enters global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and enters privileged EXEC mode.

Assigning a Secondary Path Option to Protect a Primary Path Option

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

SUMMARY STEPS

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

DETAILED STEPS

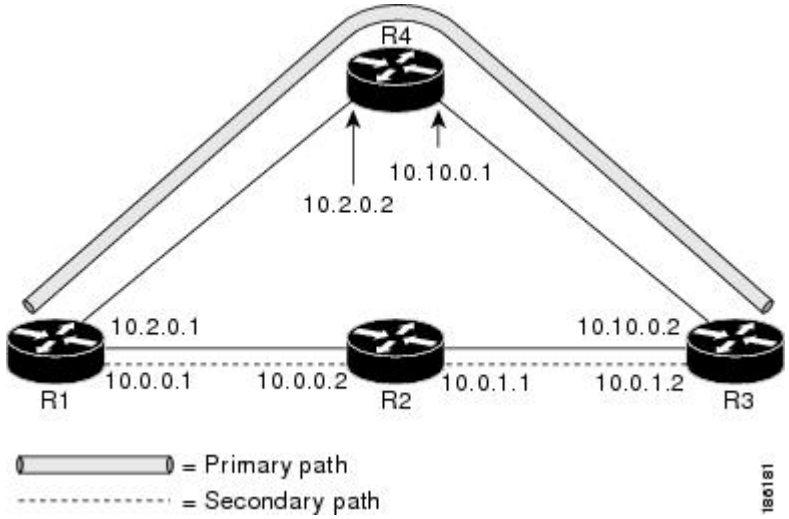
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel500`	Configures a tunnel interface and enters interface configuration mode.
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*] **Example:** `Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit name path344`	Configures a secondary path option for an MPLS TE tunnel.
Step 5	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

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 2 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
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.2.0.1  10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
 History:
  Tunnel:
    Time since created: 11 minutes, 17 seconds
    Time since path change: 8 minutes, 5 seconds
    Number of LSP IDs (Tun_Instances) used: 19
  Current LSP:
    Uptime: 8 minutes, 5 seconds
```

Step 3 **show mpls traffic-eng tunnels** *tunnel-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:

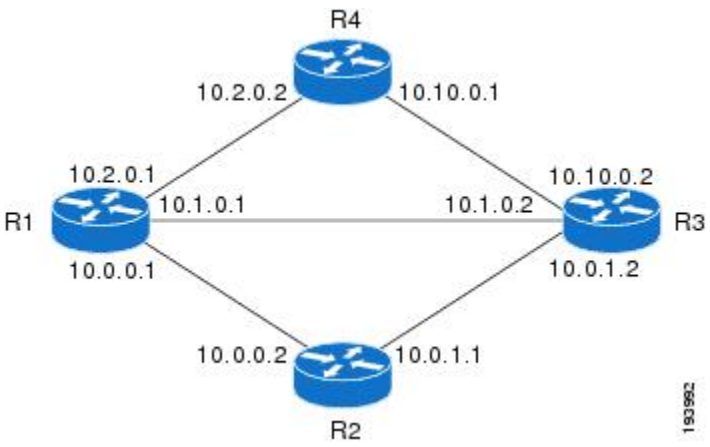
```
Router# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
 Tun ID: 500
 Header:
  State: Checkpointed  Action: Add
  Seq #: 3             Flags:  0x0
 Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10,0,0,1
  RRR path setup info
   Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
   IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
   Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
```

```
Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0
```

Enhanced Path Protection Configuration Tasks

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

Figure 3 Network Topology - Enhanced Path Protection



- Creating a Path Option List, page 11
- Assigning a Path Option List to Protect a Primary Path Option, page 13
- Verifying the Configuration of MPLS Traffic Engineering Path Protection, page 7

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

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng path-option list** [**name** *pathlist-name* | **identifier** *pathlist-number*] **Example:** `Router(config)# mpls traffic-eng path-option list name pathlist-01`	Configures a path option list, and enters path-option list configuration mode. • You can enter the following commands: **path-option**, **list**, **no**, and **exit**.
Step 4	**path-option** *number* **explicit** [**name** *pathoption-name* | **identifier***pathoption-number*] **Example:** `Router(cfg-pathoption-list)# path-option 10 explicit identifier 200`	(Optional) Specifies the name or identification number of the path option to add, edit, or delete. The *pathoption-number* value can be from 1 through 65535.
Step 5	**list** **Example:** `Router(cfg-pathoption-list)# list`	(Optional) Lists all of the path options.

	Command or Action	Purpose
Step 6	**no** [*pathoption-name* | *pathoption-number*] **Example:** `Router(cfg-pathoption-list)# no 10`	(Optional) Deletes a specified path option.
Step 7	**exit** **Example:** `Router(cfg-pathoption-list)# exit`	(Optional) Exits path-option list configuration mode and enters global configuration mode.

Assigning a Path Option List to Protect a Primary Path Option

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

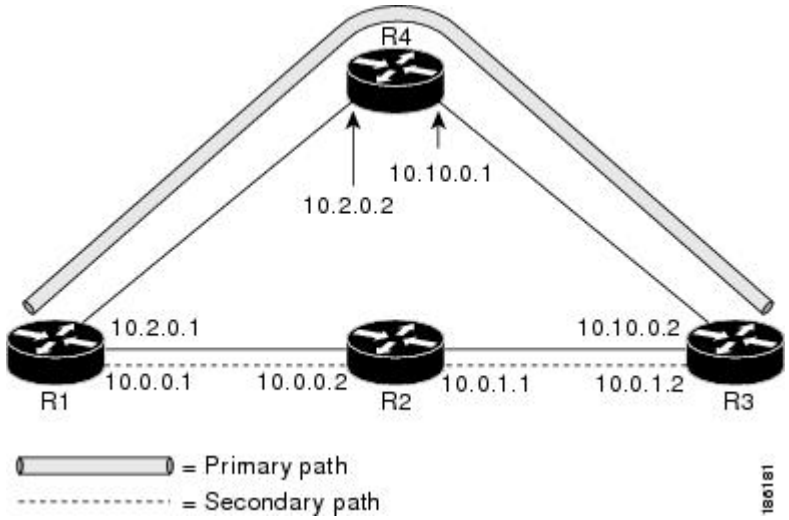
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel500`	Configures a tunnel interface and enters interface configuration mode.
Step 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*}] **Example:** `Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name pathlist-01`	Configures a path option list to protect primary path option 10.
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and enters global configuration mode.

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 4 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
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.2.0.1  10.2.0.2  10.10.0.1  10.10.0.2  10.0.0.9
 History:
  Tunnel:
    Time since created: 11 minutes, 17 seconds
    Time since path change: 8 minutes, 5 seconds
    Number of LSP IDs (Tun_Instances) used: 19
  Current LSP:
    Uptime: 8 minutes, 5 seconds
```

Step 3 **show mpls traffic-eng tunnels** *tunnel-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:

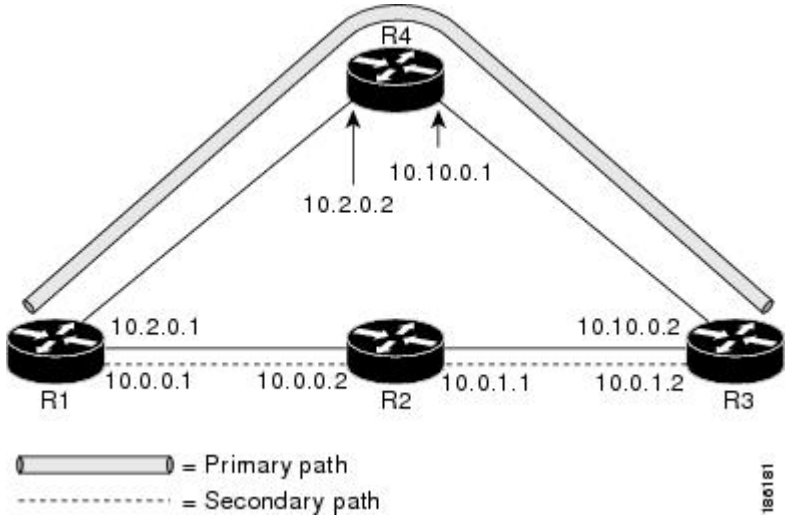
```
Router# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
 Tun ID: 500
 Header:
  State: Checkpointed  Action: Add
  Seq #: 3             Flags:  0x0
 Data:
  lsp_id: 5, bandwidth: 100, thead_flags: 0x1, popt: 1
  feature_flags: path protection active
  output_if_num: 5, output_nhop: 10,0,0,1
  RRR path setup info
   Destination: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf) flag:0x0
   IGP: ospf, IGP area: 0, Number of hops: 5, metric: 2
   Hop 0: 10.0.0.1, Id: 10.0.0.1 Router Node (ospf), flag:0x0
   Hop 1: 10.0.0.2, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 2: 10.0.1.1, Id: 10.0.0.7 Router Node (ospf), flag:0x0
   Hop 3: 10.0.1.2, Id: 10.0.0.9 Router Node (ospf), flag:0x0
   Hop 4: 10.0.0.9, Id: 10.0.0.9 Router Node (ospf), flag:0x0
```

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 5 Primary Path and Secondary Path



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

```
Router(config)# ip explicit-path name path3441 enable
Router(cfg-ip-expl-path)# index 1 next 10.0.0.1
Explicit Path name path3441:
    1: next-address 10.0.0.1
Router(cfg-ip-expl-path)# index 2 next 10.0.0.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
Router(cfg-ip-expl-path)# index 3 next 10.0.1.1
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1
Router(cfg-ip-expl-path)# index 4 next 10.0.1.2
Explicit Path name path3441:
    1: next-address 10.0.0.1
    2: next-address 10.0.0.2
    3: next-address 10.0.1.1
    4: next-address 10.0.1.2
Router(cfg-ip-expl-path)# exit
```

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
Router#
```

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

```
Router# show mpls traffic-eng tunnels tunnel500
Name: R1_t500 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
```

```
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : 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
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
 History:
  Tunnel:
   Time since created: 23 minutes, 28 seconds
   Time since path change: 50 seconds
   Number of LSP IDs (Tun_Instances) used: 44
 Current LSP:
  Uptime: 5 minutes, 24 seconds
  Selection:
 Prior LSP:
  ID: path option 10 [43]
  Removal Trigger: path error
  Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#
```

The "up" value in the Oper field of the **show mpls traffic-eng tunnels 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
   Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
   Path Weight: 20 (TE)
   Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
  History:
   Tunnel:
    Time since created: 25 minutes, 26 seconds
    Time since path change: 23 seconds
    Number of LSP IDs (Tun_Instances) used: 52
   Current LSP:
   Uptime: 26 seconds
    Selection: reoptimization
   Prior LSP:
    ID: path option 10 [44]
    Removal Trigger: reoptimization completed
R1#
```

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

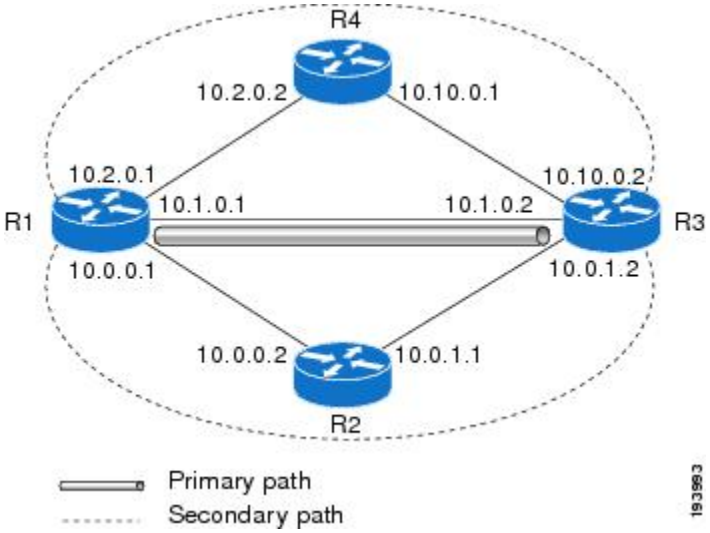
```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 52
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1   10.2.0.2
                   10.10.0.1  10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1   10.0.2
                   10.0.1.1 10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
   Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
   Metric Type: TE (default)
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

Configuration Examples for MPLS Traffic Engineering (TE): Enhanced Path Protection

Creating a Path Option List: Example

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

p Network Topology for Enhanced Path Protection



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

```
Router(config)# ip explicit-path name secondary1

Router(cfg-ip-expl-path)# index 1 next 10.0.0.2

Explicit Path name secondary1:
 1: next-address 10.0.0.2
Router(cfg-ip-expl-path)# index 2 next 10.0.1.2

Explicit Path name secondary1:
 1: next-address 10.0.0.2
 2: next-address 10.0.1.2
Router(cfg-ip-expl-path)# ip explicit-path name secondary2

Router(cfg-ip-expl-path)# index 1 next 10.2.0.2

Explicit Path name secondary2:
 1: next-address 10.2.0.2
Router(cfg-ip-expl-path)# index 2 next 10.10.0.2

Explicit Path name secondary2:
 1: next-address 10.2.0.2
 2: next-address 10.10.0.2
Router(cfg-ip-expl-path)# exit
```

In the following example a path option list of backup paths is created. You define the path option list by using the explicit paths.

```
Router(config)# mpls traffic-eng path-option list name pathlist-01

Router(cfg-pathoption-list)# path-option 10 explicit name secondary1

path-option 10 explicit name secondary1
Router(cfg-pathoption-list)# path-option 20 explicit name secondary2

path-option 10 explicit name secondary1
path-option 20 explicit name secondary2
Router(cfg-pathoption-list)# exit
```

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

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

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface tunnel 2

Router(config-if)# tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

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

```
Router# show running-config interface tunnel 2

Building configuration...
Current configuration : 296 bytes
!
interface Tunnel2
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 103.103.103.103
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name primary1
 tunnel mpls traffic-eng path-option protect 10 list name secondary-list
```

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 s**hutdown**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 (Tunnel500) Destination: 10.0.0.9
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path option 10, type explicit path344
  path option 20, type explicit path345
  Path Protection: Backup lsp in use.
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348
 Config Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
 Active Path Option Parameters:
  State: explicit path option 10 is active
  BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
 InLabel : -
 OutLabel : 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
 Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
 History:
  Tunnel:
    Time since created: 23 minutes, 28 seconds
    Time since path change: 50 seconds
    Number of LSP IDs (Tun_Instances) used: 44
 Current LSP:
  Uptime: 5 minutes, 24 seconds
  Selection:
 Prior LSP:
  ID: path option 10 [43]
  Removal Trigger: path error
  Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#
```

The "up" value in the Oper field of the **show mpls traffic-eng tunnels 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
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 20 (TE)
    Explicit Route: 10.0.0.1  10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
  History:
    Tunnel:
      Time since created: 25 minutes, 26 seconds
      Time since path change: 23 seconds
      Number of LSP IDs (Tun_Instances) used: 52
    Current LSP:
    Uptime: 26 seconds
      Selection: reoptimization
    Prior LSP:
      ID: path option 10 [44]
      Removal Trigger: reoptimization completed
R1#
```

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

```
Router# show mpls traffic-eng tunnels tunnel500 protection

R1_t500
 LSP Head, Tunnel500, Admin: up, Oper: up
 Src 10.1.1.1, Dest 10.0.0.9, Instance 52
 Fast Reroute Protection: None
 Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path:10.2.0.1   10.2.0.2
                   10.10.0.1  10.10.0.2
                   10.0.0.9
  Protect lsp path:10.0.0.1   10.0.2
                   10.0.1.1 10.0.1.2
                   10.0.0.9
  Path Protect Parameters:
    Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
```

```
  InLabel : -
  OutLabel : FastEthernet0/0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
   RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2  10.0.1.1  10.0.1.2  10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
   RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
R1#
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
MPLS traffic engineering commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
RSVP commands	*Cisco IOS Quality of Service Solutions Command Reference*
IS-IS	• *Cisco IOS IP Routing Protocols Command Reference* • Configuring a Basic IS-IS Network
OSPF	• *Cisco IOS IP Routing Protocols Command Reference* • Configuring OSPF
ISSU	Cisco IOS XE In Service Software Upgrade Support
NSF/SSO	• Cisco Nonstop Forwarding • Stateful Switchover

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

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 1 Feature Information for MPLS Traffic Engineering (TE): Path Protection

Feature Name	Releases	Feature Information
MPLS Traffic Engineering (TE): Path Protection	12.0(30)S 12.2(18)SXD1 12.2(33)SRC 12.4(20)T 12.2(33)SRE	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.