Configuring MPLS TE Path Protection

This chapter describes how to configure Multiprotocol Label Switching (MPLS) path protection for traffic engineering (TE) on Cisco NX-OS devices.

This chapter includes the following sections:

- Finding Feature Information, page 19-270
- Information About MPLS TE Path Protection, page 19-270
- Licensing Requirements for MPLS TE Path Protection, page 19-272
- Prerequisites for MPLS TE Path Protection, page 19-272
- Guidelines and Limitations for MPLS TE Path Protection, page 19-273
- Configuring MPLS TE Path Protection, page 19-273
- Verifying the MPLS TE Path Protection Configuration, page 19-278
- Verifying the Enhanced Path Protection Configuration, page 19-280
- Additional References for MPLS TE Path Protection, page 19-295
- Feature History for MPLS TE Path Protection, page 19-296

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 “New and Changed Information” chapter or the Feature History table below.

Information About MPLS TE Path Protection

Path protection provides an end-to-end failure recovery function (full path protection) for MPLS TE tunnels. Cisco NX-OS supports regular path protection and enhanced path protection, which is the ability to configure up to eight secondary path options for a given primary path option.

This section includes the following topics:

- Path Protection, page 19-271
- Enhanced Path Protection, page 19-271
Path Protection

A secondary label switched path (LSP) is configured and established to provide failure protection for the 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

- Single area
  - Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)
- Interarea
  - Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)
- Inter-AS
  - Border Gateway Protocol (BGP), both external BGP (eBGP,) and static

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

- Path error or resv tear from RSVP signaling
- 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, online insertion and removal (OIR), and so forth

An alternate recovery function 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 is affected by delay factors such as propagation delay or switch fabric latency.

Enhanced Path Protection

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

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

Cisco In Service Software Upgrade (ISSU) allows you to perform a Cisco NX-OS software upgrade or downgrade while the system continues to forward packets. ISSU takes advantage of the Cisco NX-OS high availability infrastructure (Cisco nonstop forwarding [NSF] with stateful switchover [SSO] and hardware redundancy) and eliminates the downtime that is associated with software upgrades or version changes by allowing changes while the system remains in service. Cisco ISSU lowers the impact that planned maintenance activities have on network service availability; there is less downtime and better access to critical systems.

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

NSF/SSO

Cisco NSF with SSO provides continuous packet forwarding, even during a network processor hardware or software failure.

Path protection 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 if there is a failure along the primary path. Only information associated with one of those LSPs, the one that is currently carrying traffic, is synchronized to the standby system. On recovery, the standby system 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 provided path protection is resignal after the TE recovery period is complete. This process does not impact the traffic on the tunnel because the secondary LSP was not carrying traffic.

Licensing Requirements for MPLS TE Path Protection

<table>
<thead>
<tr>
<th>Product</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco NX-OS</td>
<td>MPLS TE path protection requires an MPLS license. For a complete explanation of the NX-OS licensing scheme and how to obtain and apply licenses, see the <em>Cisco NX-OS Licensing Guide</em>.</td>
</tr>
</tbody>
</table>

Prerequisites for MPLS TE Path Protection

Path protection has the following prerequisites:

- The MPLS TE feature must be enabled. MPLS TE can be enabled or disabled by the `no feature mpls traffic-eng` command and is disabled by default. See the “Configuring MPLS TE” section on page 11-145.
- Configure a TE tunnel with a primary path option by using the `path-option` command.
Guidelines and Limitations for MPLS TE Path Protection

Path protection has the following configuration guidelines and limitations:

- The secondary path will not be signaled with the FRR flag.
- Dynamic diverse paths are not supported. You must configure an explicit path for the secondary LSP that avoids using any shared links with the primary LSP.
- Do not use link and node protection with path protection on the headend router.

Configuring MPLS TE Path Protection

This section includes the following topics:

- Configuring Explicit Paths for Secondary Paths, page 19-273
- Assigning a Secondary Path Option to Protect a Primary Path Option, page 19-274

These tasks are described in the following sections and are shown in Figure 19-1.

Figure 19-1   Network Topology—Path Protection

Configuring Explicit Paths for Secondary Paths

You can 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.

Prerequisites

You must enable the MPLS TE feature (see the “Configuring MPLS TE” section on page 11-145). Ensure that you are in the correct VDC (or use the switchto vdc command).
Chapter 19  Configuring MPLS TE Path Protection

SUMMARY STEPS

1. configure terminal
2. mpls traffic-eng configuration
3. [no] explicit-path {name path-name | identifier number}
4. index index command ip-address

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
</tr>
<tr>
<td>Example:</td>
<td>switch# configure terminal</td>
</tr>
<tr>
<td></td>
<td>switch(config)#</td>
</tr>
<tr>
<td>Step 2</td>
<td>mpls traffic-eng configuration</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config)# mpls traffic-eng configuration</td>
</tr>
<tr>
<td></td>
<td>switch(config-te)#</td>
</tr>
<tr>
<td>Step 3</td>
<td>[no] explicit-path {name path-name</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-te)# explicit-path name path1223</td>
</tr>
<tr>
<td></td>
<td>switch(config-te-expl-path)</td>
</tr>
<tr>
<td>Step 4</td>
<td>index index command ip-address</td>
</tr>
<tr>
<td>Example:</td>
<td>switch(config-te-expl-path)# index 10</td>
</tr>
<tr>
<td></td>
<td>next-address 10.0.0.2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Assigning a Secondary Path Option to Protect a Primary Path Option

You can 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.

Prerequisites

You must have the MPLS TE feature enabled (see the “Configuring MPLS TE” section on page 11-145). Ensure that you are in the correct VDC (or use the switchto vdc command).

SUMMARY STEPS

1. configure terminal
2. interface tunnel-te number
3. **path-option protect** number explicit {identifier path-number | name path-name} [attributes lsp-attributes | bandwidth kbps | lockdown] [verbatim]

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch# configure terminal</td>
<td></td>
</tr>
<tr>
<td>switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface tunnel-te number</td>
<td>Enters TE interface configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config)# interface tunnel-te 1</td>
<td></td>
</tr>
<tr>
<td>switch(config-if-te)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> path-option protect number explicit {identifier path-number</td>
<td>name path-name} [attributes lsp-attributes</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>switch(config-if-te)# path-option protect 10</td>
<td></td>
</tr>
<tr>
<td>explicit name path344</td>
<td></td>
</tr>
</tbody>
</table>

### Enhanced Path Protection Configuration Tasks

This section includes the following topics:

- Creating a Path Option List, page 19-276
- Assigning a Path Option List to Protect a Primary Path Option, page 19-277

These tasks are described in the following sections and are shown in **Figure 19-2**.

**Figure 19-2**       *Network Topology - Enhanced Path Protection*
Creating a Path Option List

In enhanced path protection you can create and assign a path option list.

Note

To use a secondary path instead, follow the steps in the “Configuring Explicit Paths for Secondary Paths” section on page 19-273.

SUMMARY STEPS

1. configure terminal
2. interface tunnel-te number
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. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface tunnel-te number</td>
<td>Enters TE interface configuration mode.</td>
</tr>
<tr>
<td>Example: switch(config)# interface tunnel-te 1 switch(config-if-te)#</td>
<td>The <em>number</em> argument identifies the tunnel number to be configured.</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>Example: switch(config)# mpls traffic-eng path-option list name pathlist-01</td>
<td>You can enter the following commands: <em>path-option, list, no, and exit</em>.</td>
</tr>
<tr>
<td><strong>Step 4</strong> path-option number explicit [name pathoption-name</td>
<td>identifier pathoption-number]</td>
</tr>
<tr>
<td>Example: switch(cfg-pathoption-list)# path-option 10 explicit identifier 200</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> list</td>
<td>(Optional) Lists all of the path options.</td>
</tr>
<tr>
<td>Example: switch(cfg-pathoption-list)# list</td>
<td></td>
</tr>
</tbody>
</table>
### Assigning a Path Option List to Protect a Primary Path Option

You can assign a path option list in case there is a link or node failure along a path and all interfaces in your network are not protected. See Figure 19-2.

#### SUMMARY STEPS

1. `configure terminal`
2. `interface tunnel-te number`
3. `path-option protect number [attributes lsp-attributes | bandwidth {kbps | subpool kbps} | explicit {identifier path-number | name path-name} | list {name pathlist-name | identifier pathlist-identifier}]`
4. `end`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: switch# configure terminal switch(config)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> interface tunnel-te number</td>
<td>Enters TE interface configuration mode. The <em>number</em> argument identifies the tunnel number to be configured.</td>
</tr>
<tr>
<td>Example: switch(config)# interface tunnel-te 500 switch(config-if-te)#</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> path-option protect number [attributes lsp-attributes</td>
<td>bandwidth {kbps</td>
</tr>
<tr>
<td>Example: switch(config-if-te)# path-option protect 10 list name pathlist-01</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> end</td>
<td>Exits to EXEC mode.</td>
</tr>
<tr>
<td>Example: switch(config-if-te)# end switch#</td>
<td></td>
</tr>
</tbody>
</table>
Verifying the MPLS TE Path Protection Configuration

You can display the path protection configuration. Steps 1 and 2 refer to Figure 19-3.

Figure 19-3 Network Topology Verification

![Network Topology Verification Diagram]

To display path protection for verification, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running interface tunnel-te number</code></td>
<td>Displays the configuration of the primary path and the protection path options.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels tunnel-te number</code></td>
<td>Displays tunnel path information.</td>
</tr>
<tr>
<td><code>show mpls traffic-eng tunnels tunnel-te number protection</code></td>
<td>Displays the status of both LSPs (primary path and protected path), when the <code>protection</code> keyword is specified.</td>
</tr>
</tbody>
</table>

**Note** Deleting a primary path option has the same effect as shutting down a link. Traffic moves to the protected path.

**Examples**

The following example shows how to display the configuration of the primary path and protection path options.

```
switch# show running interface tunnel-te500
Building configuration...
Current configuration : 497 bytes
```

To show the status of both LSPs (primary path and protected path), use the `show mpls traffic-eng tunnels` command with the `protection` keyword.
### Chapter 19      Configuring MPLS TE Path Protection

#### Verifying the MPLS TE Path Protection Configuration

```
interface Tunnel-te500
  ip unnumbered Loopback0
destination 10.0.0.9
autoroute announce
priority 7 7
bandwidth 100
path-option 10 explicit name path344
path-option 20 explicit name path345
path-option protect 10 explicit name path3441
path-option protect 20 explicit name path348
end
```

The following example shows how to display tunnel path information.

```
The command output shows no common links or nodes.
```

**Note**

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

```
switch# show mpls traffic-eng tunnels tunnel-te500
Name: R1_t500 (Tunnel-te500) Destination: 10.0.0.9
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit path344 (Basis for Setup, path weight 20)
  path option 20, type explicit path345
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
  path protect option 20, type explicit path348

Config Parameters:
  Bandwidth: 100 kb/s (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
  auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

  InLabel : -
  OutLabel : Ethernet1/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 19
RSVP Path Info:
  My Address: 10.2.0.1
  Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  Shortest Unconstrained Path Info:
    Path Weight: 20 (TE)
    Explicit Route: 10.2.0.1 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
    History:
      Tunnel:
```
Chapter 19 Configuring MPLS TE Path Protection

Verifying the MPLS TE Path Protection Configuration

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

The following example shows how to display the status of both LSPs (primary path and protected path) when the protection keyword is specified.

Note
Deleting a primary path option has the same effect as shutting down a link. Traffic moves to the protected path.

The command output shows that both primary LSP and secondary LSP are up and protection is enabled:

```
switch# show mpls traffic-eng tunnels tunnel-te500 protection

R1_t500
LSP Head, Tunnel-te500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 19
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path: 10.2.0.1 10.2.0.2
  10.10.0.1 10.10.0.2
  10.0.0.9
  Protect lsp path: 10.0.0.1 10.0.0.2
  10.0.1.1 10.0.1.2
  10.0.0.9
Path Protect Parameters:
  Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  InLabel: -
  OutLabel: Ethernet0/0, 16
RSVP Signalling Info:
  Src 10.1.1.1, Dest 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 example shows that the primary LSP is down and that the secondary LSP is up and is carrying traffic:

```
switch# show mpls traffic-eng tunnels tunnel-te500 protection

R1_t500
LSP Head, Tunnel-te500, 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.
```

Verifying the Enhanced Path Protection Configuration

To verify the enhanced path protection configuration, refer to Figure 19-4 and perform the following steps.
SUMMARY STEPS

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

DETAILED STEPS

Step 1  
`show running interface tunnel-te number`

This command shows the configuration of the path option and backup path option.

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

switch# show running interface tunnel-te2

Building configuration..

Current configuration : 296 bytes

! interface Tunnel-te2
  ip unnumbered Loopback0
  destination 10.10.0.2
  autoroute announce
  path-option 10 explicit name primary1
Step 2  show mpls traffic-eng tunnels tunnel-te number

This command shows tunnel path information.

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

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

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

switch# show mpls traffic-eng tunnels tunnel-te2

Name: iou-100_t2 (Tunnel-te2) Destination: 10.10.0.2
 Status: 
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
  Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 188
RSVP Path Info:
  My Address: 10.1.0.1
  Explicit Route: 10.1.0.2 10.10.0.2
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 10 (TE)
  Explicit Route: 10.1.0.1 10.1.0.2 10.10.0.2
History:
  Tunnel:
    Time since created: 1 hours, 34 minutes
    Time since path change: 1 minutes, 50 seconds
    Number of LSP IDs (Tun_Instances) used: 188
  Current LSP:
    Uptime: 1 minutes, 50 seconds
    Prior LSP:
      ID: path option 10 [44]
      Removal Trigger: label reservation removed

Step 3  show mpls traffic-eng tunnels tunnel-te number [brief] [protection]

Use this command, with the protection keyword specified, to show the status of both LSPs (that is, both the primary path and the protected path).
Verifying the MPLS TE Path Protection Configuration

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

```
switch# show mpls traffic-eng tunnels tunnel-te2 protection
iou-100_t2
LSP Head, Tunnel-te2, Admin: up, Oper: up
Src 100.100.100.100, Dest 10.10.0.2, Instance 188
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
  Primary lsp path: 10.1.0.1 10.1.0.2
  Protect lsp path: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.10.0.2
Path Protect Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  InLabel : -
  OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
  Src 100.100.100.100, Dst 10.10.0.2, Tun_Id 2, Tun_Instance 189
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.10.0.2
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
```

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

```
switch# show mpls traffic-eng tunnels tunnel-te500 protection
R1_t500
LSP Head, Tunnel-te500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 27
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
```

**Step 4**

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

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

```
switch# show ip rsvp high-availability database lsp-head
LSP_HEAD WRITE DB
  Tun ID: 2
Header:
  State: Checkpointed Action: Add
  Seq #: 2 Flags: 0x0
Data:
  lsp_id: 6, bandwidth: 0, thead_flags: 0x1, popt: 10
  feature flags: none
  output_if_num: 31, output_nhop: 10.1.0.2
  RRR path setup info
    Destination: 10.10.0.2, Id: .10.10.0.2 Router Node (ospf) flag:0x0
```
Configuration Examples for MPLS TE Path Protection

This section includes the following topics:

- Example: Configuring Explicit Paths for Secondary Paths, page 19-284
- Example: Assigning a Secondary Path Option to Protect a Primary Path Option, page 19-285
- Example: Configuring Tunnels Before and After Path Protection, page 19-285

Example: Configuring Explicit Paths for Secondary Paths

Figure 19-5 shows a primary path and a secondary path. If there is a failure, the secondary path is used.

Figure 19-5  Primary Path and Secondary Path

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

```
switch(config)# mpls traffic-eng configuration
switch(config-te)# explicit-path name path3441
switch(config-te-expl-path)# index 1 next-address 10.0.0.1
Explicit Path name path3441:
  1: next-address 10.0.0.1
switch(config-te-expl-path)# index 2 next-address 10.0.0.2
Explicit Path name path3441:
  1: next-address 10.0.0.1
  2: next-address 10.0.0.2
```
Example: Assigning a Secondary Path Option to Protect a Primary Path Option

The following example shows that a TE tunnel is configured:

```
switch# configure terminal
switch(config)# interface tunnel-te500
switch(config-if-te)# path-option protect 10 explicit name path344
```

The following example 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.

```
switch# show running interface tunnel-te500
Building configuration...

Current configuration : 497 bytes
!
interface Tunnel-te500
  ip unnumbered Loopback0
  destination 10.0.0.9
  autoroute announce
  priority 7 7
  bandwidth 100
  path-option 10 explicit name path344
  path-option 20 explicit name path345
  path-option protect 10 explicit name path3441
  path-option protect 20 explicit name path348

end
```

Example: Configuring Tunnels Before and After Path Protection

The following example shows information about the primary (protected) path. The following sample output shows that path protection has been configured:

```
switch# show mpls traffic-eng tunnels tunnel-te500
Name: R1_t500 (Tunnel-te500)  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
```
Chapter 19 Configuring MPLS TE Path Protection

Configuration Examples for MPLS TE Path Protection

Config Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based auto-bw: disabled
Active Path Option Parameters:
State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet1/0, 16
RSVP Signalling Info:
Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 43
RSVP Path Info:
My Address: 10.2.0.1
Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
Record Route: NONE
Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
Record Route: NONE
Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9

History:
Tunnel:
Time since created: 18 minutes, 22 seconds
Time since path change: 19 seconds
Number of LSP IDs (Tun_Instances) used: 43
Current LSP:
Uptime: 22 seconds
Selection: reoptimization
Prior LSP:
ID: path option 10 [27]
Removal Trigger: reoptimization completed

The following example 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.

```
switch# show mpls traffic-eng tunnels tunnel-te500 protection

R1_t500
LSP Head, Tunnel500, Admin: up, Oper: up
Src 10.1.1.1, Dest 10.0.0.9, Instance 43
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path:10.2.0.1 10.2.0.2
10.10.0.1 10.10.0.2
10.0.0.9
Protect lsp path:10.0.0.1 10.0.0.2
10.0.1.1 10.0.1.2
10.0.0.9
Path Protect Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet0/0, 16
RSVP Signalling Info:
Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
RSVP Path Info:
```
Configuration Examples for MPLS TE Path Protection

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 example shows how to shut down the interface to use path protection:

switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface e1/0
switch(config-if)# shutdown

The following example shows that the protection path is used and the primary path is down:

switch# show mpls traffic-eng tunnels tunnel-te500
Name: R1_t500 (Tunnel-te500) Destination: 10.0.0.9
Status: Admin: up Oper: up Path: valid Signalling: connected
path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
path option 10, type explicit path344
path option 20, type explicit path345
Path Protection: Backup lsp in use.
path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
path protect option 20, type explicit path348

Config Parameters:
Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
auto-bw: disabled
Active Path Option Parameters:
State: explicit path option 10 is active
BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet0/0, 17
RSVP Signalling Info:
  Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 44
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
  Record Route: NONE
  Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
Shortest Unconstrained Path Info:
Path Weight: 20 (TE)
Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
History:
  Tunnel:
    Time since created: 23 minutes, 28 seconds
    Time since path change: 50 seconds
    Number of LSP IDs (Tun_Instances) used: 44
  Current LSP:
    Uptime: 5 minutes, 24 seconds
    Selection:
    Prior LSP:
    ID: path option 10 [43]
Removal Trigger: path error
    Last Error: PCALC:: Explicit path has unknown address, 10.2.0.1
R1#

The following example shows that protection is enabled:

```
switch# show mpls traffic-eng tunnels tunnel-te500 protection
R1_t500
LSP Head, Tunnel-te500, 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 following example shows that the interface is up again and the primary path is activated:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface ethernet1/0
switch(config-if)# no shutdown
R1#
```

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

```
switch# show mpls traffic-eng tunnels tunnel-te500
Name: R1_t500 (Tunnel-te500) Destination: 10.0.0.9
Status:
    Admin: up Oper: up Path: valid Signalling: connected
path option 10, type explicit path344 (Basis for Setup, path weight 20)
path option 20, type explicit path345
Path Protection: 0 Common Link(s), 0 Common Node(s)
path protect option 10, type explicit path3441 (Basis for Protect, path weight 20)
path protect option 20, type explicit path348
Config Parameters:
    Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: enabled LockDown: disabled Loadshare: 100 bw-based
    auto-bw: disabled
    Active Path Option Parameters:
        State: explicit path option 10 is active
        BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : Ethernet1/0, 16
RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 52
RSVP Path Info:
    My Address: 10.2.0.1
    Explicit Route: 10.2.0.2 10.10.0.1 10.10.0.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
    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:
```
The following example shows that Tunnel-te500 is protected and after a failure, the primary LSP is protected:

```plaintext
switch# show mpls traffic-eng tunnels tunnel-te500 protection
R1_t500
  LSP Head, Tunnel-te500, Admin: up, Oper: up
  Src 10.1.1.1, Dest 10.0.0.9, Instance 52
  Fast Reroute Protection: None
  Path Protection: 0 Common Link(s), 0 Common Node(s)
    Primary lsp path: 10.2.0.1 10.2.0.2
      10.10.0.1 10.10.0.2
      10.0.0.9
    Protect lsp path: 10.0.0.1 10.0.2
      10.0.1.1 10.0.1.2
      10.0.0.9
  Path Protect Parameters:
    Bandwidth: 100 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    InLabel : -
    OutLabel : Ethernet0/0, 16
  RSVP Signalling Info:
    Src 10.1.1.1, Dst 10.0.0.9, Tun_Id 500, Tun_Instance 53
  RSVP Path Info:
    My Address: 10.0.0.1
    Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 10.0.0.9
    Record Route: NONE
    Tspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=100 kbits, burst=1000 bytes, peak rate=100 kbits
```

Examples of Enhanced Path Protection

This section includes the following topics:

- Example: Creating a Path Option List, page 19-289
- Example: Assigning a Path Option List to Protect a Primary Path Option, page 19-291
- Example: Configuring Tunnels Before and After Path Protection, page 19-291

Example: Creating a Path Option List

Figure 19-6 shows the network topology for enhanced path protection.
The following example shows how to configure two explicit paths named `secondary1` and `secondary2`.

```plaintext
switch(config)# ip explicit-path name secondary1
switch(config-te-expl-path)# index 1 next 10.0.0.2
Explicit Path name secondary1:
1: next-address 10.0.0.2

switch(config-te-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

switch(config-te-expl-path)# ip explicit-path name secondary2
switch(config-te-expl-path)# index 1 next 10.2.0.2
Explicit Path name secondary2:
1: next-address 10.2.0.2

switch(config-te-expl-path)# index 2 next 10.0.0.2
Explicit Path name secondary2:
1: next-address 10.0.0.2
2: next-address 10.0.1.2

switch(config-te-expl-path)# exit
```

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

```plaintext
switch(config)# mpls traffic-eng
switch(config-te)# path-option list name pathlist-01
switch(cfg-pathoption-list)# path-option 10 explicit name secondary1
path-option 10 explicit name secondary1

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

switch(cfg-pathoption-list)# exit
```
Example: Assigning a Path Option List to Protect a Primary Path Option

The following example shows that a traffic engineering tunnel is configured:

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

The following example shows that path protection has been configured. Tunnel 2 has path option 10 using path primary1 and protected by secondary-list.

```
switch# 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 following example shows information about the primary (protected) path. The following sample output shows that path protection has been configured:

```
switch# show mpls traffic-eng tunnels tunnel 2
Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 10, type explicit primary1 (Basis for Setup, path weight 10)
  Path Protection: 0 Common Link(s), 0 Common Node(s)
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based
  auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled
InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 11
RSVP Path Info:
  My Address: 10.1.0.1
  Explicit Route: 10.1.0.2 103.103.103.103
  Record Route: NONE
  Tspspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
  RSVP Resv Info:
    Record Route: NONE
    Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
```
Shortest Unconstrained Path Info:
Path Weight: 10 (TE)
Explicit Route: 10.1.0.1 10.1.0.2 103.103.103.103
History:
Tunnel:
  Time since created: 24 minutes, 15 seconds
  Time since path change: 23 minutes, 30 seconds
  Number of LSP IDs (Tun_Instances) used: 11
  Current LSP:
    Uptime: 23 minutes, 30 seconds

The following shows information about the secondary path. Tunnel 2 is protected.

```
switch# show mpls traffic-eng tunnels tunnel 2 protection
```

Router_t2
LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 11
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path: 10.1.0.1 10.1.0.2 103.103.103.103
Protect lsp path: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
Path Protect Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  InLabel : -
  OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 20
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits

The following example shows how to shut down the interface to use path protection:

```
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface e7/0
switch(config-if)# shutdown
switch(config-if)# end
```

The following example shows that the protection path is used, and the primary path is down:

```
switch# show mpls traffic-eng tunnels tunnel 2
```

Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
  path option 10, type explicit primary1
  Path Protection: Backup lsp in use.
  path protect option 10, type list name secondary-list
  Inuse path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)
Configuration Examples for MPLS TE Path Protection

Config Parameters:
  Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
  AutoRoute announce: enabled LockDown: disabled Loadshare: 0 bw-based auto-bw: disabled
  Active Path Option Parameters:
    State: list path option 10 is active
    BandwidthOverride: disabled LockDown: disabled Verbatim: disabled

InLabel : -
OutLabel : Ethernet5/0, 16
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 20
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fs pec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 20 (TE)
  Explicit Route: 10.0.0.1 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103

History:
  Tunnel:
    Time since created: 32 minutes, 27 seconds
    Time since path change: 1 minutes, 7 seconds
    Number of LSP IDs (Tun_Instances) used: 20
  Current LSP:
    Uptime: 8 minutes, 56 seconds
    Selection:
    Prior LSP:
      ID: path option 10 [11]
      Removal Trigger: path error
      Last Error: PCALC:: No addresses to connect 100.100.100.100 to 10.1.0.2

The following example shows that protection is enabled.

```
switch# show mpls traffic-eng tunnels tunnel 2 protection

Router_t2
LSP Head, Tunnel2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 20
Fast Reroute Protection: None
Path Protection: Backup lsp in use.
```

The following example shows that the interface is up again and the primary path is activated.

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config-if)# interface ethernet7/0
switch(config-if)# no shutdown
switch(config-if)# end
```

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

```
switch# show mpls traffic-eng tunnels tunnel 2

Name: Router_t2 (Tunnel2) Destination: 103.103.103.103
Status:
Chapter 19  Configuring MPLS TE Path Protection

Configuration Examples for MPLS TE Path Protection

Admin: up  Oper: up  Path: valid  Signalling: connected
path option 10, type explicit primary1 (Basis for Setup, path weight 10)
Path Protection: 0 Common Link(s), 0 Common Node(s)
path protect option 10, type list name secondary-list
In use path-option 10, type explicit secondary1 (Basis for Protect, path weight 20)

Config Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
AutoRoute announce: enabled  LockDown: disabled  Loadshare: 0 bw-based
auto-bw: disabled
Active Path Option Parameters:
State: explicit path option 10 is active
Bandwidth Override: disabled  LockDown: disabled  Verbatim: disabled

InLabel : -
OutLabel : Ethernet7/0, implicit-null
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 39
RSVP Path Info:
  My Address: 10.1.0.1
  Explicit Route: 10.1.0.2 103.103.103.103
  Record Route: NONE
  Tspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=0 kbits, burst=1000 bytes, peak rate=0 kbits
Shortest Unconstrained Path Info:
  Path Weight: 10 (TE)
  Explicit Route: 10.1.0.1 10.1.0.2 103.103.103.103
History:
  Tunnel:
    Time since created: 40 minutes, 59 seconds
    Time since path change: 1 minutes, 24 seconds
    Number of LSP IDs (Tun_Instances) used: 39
Current LSP:
  Uptime: 1 minutes, 27 seconds
  Selection: reoptimization
Prior LSP:
  ID: path option 10 [20]
  Removal Trigger: reoptimization completed

switch# show mpls traffic-eng tunnels tunnel 2 protection

Router_t2
LSP Head, Tunnel 2, Admin: up, Oper: up
Src 100.100.100.100, Dest 103.103.103.103, Instance 39
Fast Reroute Protection: None
Path Protection: 0 Common Link(s), 0 Common Node(s)
Primary lsp path: 10.1.0.1 10.1.0.2
  103.103.103.103
Protect lsp path: 10.0.0.1 10.0.0.2
  10.0.1.1 10.0.1.2
  103.103.103.103
Path Protect Parameters:
Bandwidth: 0 kbps (Global) Priority: 7 7 Affinity: 0x0/0xFFFF
Metric Type: TE (default)
InLabel : -
OutLabel : Ethernet5/0, 17
RSVP Signalling Info:
  Src 100.100.100.100, Dst 103.103.103.103, Tun_Id 2, Tun_Instance 40
RSVP Path Info:
  My Address: 10.0.0.1
  Explicit Route: 10.0.0.2 10.0.1.1 10.0.1.2 103.103.103.103

Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide
The following example shows the contents of the RSVP high availability read and write databases used in TE.

```plaintext
switch# show ip rsvp high-availability database lsp-head
```

**LSP HEAD WRITE DB**

- **Tun ID**: 2
- **Header**:
  - **State**: Checkpointed
  - **Action**: Modify
  - **Seq #**: 17
  - **Flags**: 0x0
- **Data**:
  - **lsp_id**: 39
  - **bandwidth**: 0
  - **thead_flags**: 0x1
  - **popt**: 10
  - **feature flags**: none
  - **output_if_num**: 31
  - **output_nhhop**: 10.1.0.2

**RRR path setup info**

- **Destination**: 103.103.103.103
- **Id**: 103.103.103.103
- **Router Node (ospf)**
- **flag**: 0x0
- **IGP**: ospf
- **IGP area**: 0
- **Number of hops**: 3
- **metric**: 10
- **Hop 0**: 10.1.0.1
- **Id**: 100.100.100.100
- **Router Node (ospf)**
- **flag**: 0x0
- **Hop 1**: 10.1.0.2
- **Id**: 103.103.103.103
- **Router Node (ospf)**
- **flag**: 0x0
- **Hop 2**: 103.103.103.103
- **Id**: 103.103.103.103
- **Router Node (ospf)**
- **flag**: 0x0

**LSP HEAD READ DB**

---

### Additional References for MPLS TE Path Protection

The following sections provide references related to the MPLS TE path protection feature.
Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS TE commands</td>
<td>Cisco NX-OS Multiprotocol Label Switching Command Reference</td>
</tr>
<tr>
<td>RSVP</td>
<td>Cisco NX-OS Quality of Service Commands</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Cisco NX-OS Unicast Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>Configuring a Basic IS-IS Network</td>
</tr>
<tr>
<td>OSPF</td>
<td>Cisco NX-OS Unicast Routing Protocols Command Reference</td>
</tr>
<tr>
<td></td>
<td>Configuring OSPF</td>
</tr>
<tr>
<td>ISSU</td>
<td>ISSU MPLS Clients</td>
</tr>
<tr>
<td>NSF/SSO</td>
<td>Cisco NX-OS High Availability and Redundancy Guide</td>
</tr>
</tbody>
</table>

MIBs

<table>
<thead>
<tr>
<th>MIB</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CISCO-IETF-FRR-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases,</td>
</tr>
<tr>
<td>• MPLS TE-STD-MIB</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>

Feature History for MPLS TE Path Protection

Table 19-1 lists the release history for this feature.

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Path protection</td>
<td>5.2(1)</td>
<td>This feature was introduced.</td>
</tr>
</tbody>
</table>