

MPLS Traffic Engineering-Autotunnel Primary and Backup

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

A router with primary one-hop autotunnels and backup autotunnels can be configured with stateful switchover (SSO) redundancy.

- Prerequisites for MPLS Traffic Engineering-Autotunnel Primary and Backup, on page 1
- Restrictions for MPLS Traffic Engineering-Autotunnel Primary and Backup, on page 1
- Information About MPLS Traffic Engineering-Autotunnel Primary and Backup, on page 2
- How to Configure MPLS Traffic Engineering Autotunnel Primary and Backup, on page 8
- Configuration Examples for MPLS Traffic Engineering-Autotunnel Primary and Backup, on page 11
- Additional References, on page 16
- Feature Information for MPLS Traffic Engineering-Autotunnel Primary and Backup, on page 17
- Glossary, on page 18

Prerequisites for MPLS Traffic Engineering-Autotunnel Primary and Backup

- Configure TE on the routers.

Restrictions for MPLS Traffic Engineering-Autotunnel Primary and Backup

- You cannot configure a static route to route traffic over TE autotunnels. For autotunnels, you should use only the autoroute for tunnel selection.

Information About MPLS Traffic Engineering-Autotunnel Primary and Backup

Overview of MPLS Traffic Engineering-Autotunnel Primary and Backup

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature has the following features:

- Backup autotunnel-Enables a router to dynamically build backup tunnels.
- Primary one-hop autotunnel-Enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

If no backup tunnels exist, the following types of backup tunnels are created:

- Next hop (NHOP)
- Next-next hop (NNHOP)

Benefits of MPLS Traffic Engineering-Autotunnel Primary and Backup Feature

- Backup tunnels are built automatically, eliminating the need for users to preconfigure each backup tunnel and then assign the backup tunnel to the protected interface.
- The dynamic creation of one-hop primary tunnels eliminates the need to configure an MPLS TE tunnel with the Fast Reroute (FRR) option for the tunnel to be protected.
- Protection is expanded; FRR does not protect IP traffic that is not using the TE tunnel or Label Distribution Protocol (LDP) labels that are not using the TE tunnel.

MPLS Traffic Engineering

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

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

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

MPLS Traffic Engineering Backup Autotunnels

MPLS backup autotunnels protect fast reroutable TE label switched paths (LSPs). Without MPLS backup autotunnels to protect a LSP you had to do the following:

- Preconfigure each backup tunnel.
- Assign the backup tunnels to the protected interfaces.

An LSP requests backup protection from Resource Reservation Protocol (RSVP) FRR in the following situations:

- Receipt of the first RSVP Resv message
- Receipt of an RSVP path message with the protection attribute after the LSP has been established without the protection attribute
- Detection that a Record Route Object (RRO) changed

If there was no backup tunnel protecting the interface used by the LSP, the LSP remained unprotected.

Backup autotunnels enable a router to dynamically build backup tunnels when they are needed. This prevents you from having to build MPLS TE tunnels statically.

Backup tunnels may not be available for the following reasons:

- Static backup tunnels are not configured.
- Static backup tunnels are configured, but cannot protect the LSP. The backup tunnel may not have enough available bandwidth, the tunnel may protect a different pool, or the tunnel may be down.

If a backup tunnel is not available, the following two backup tunnels are created dynamically:

- NHOP--Protects against link failure
- NNHOP--Protects against node failure

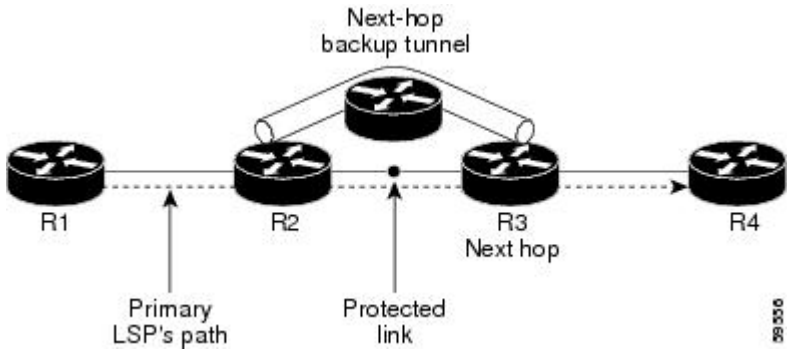
Note At the penultimate hop, only an NHOP backup tunnel is created.

Note If two LSPs share the same output interface and NHOP, three (not four) backup tunnels are created. They share an NHOP backup tunnel.

Link Protection

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

Figure 1: NHOP Backup Tunnel

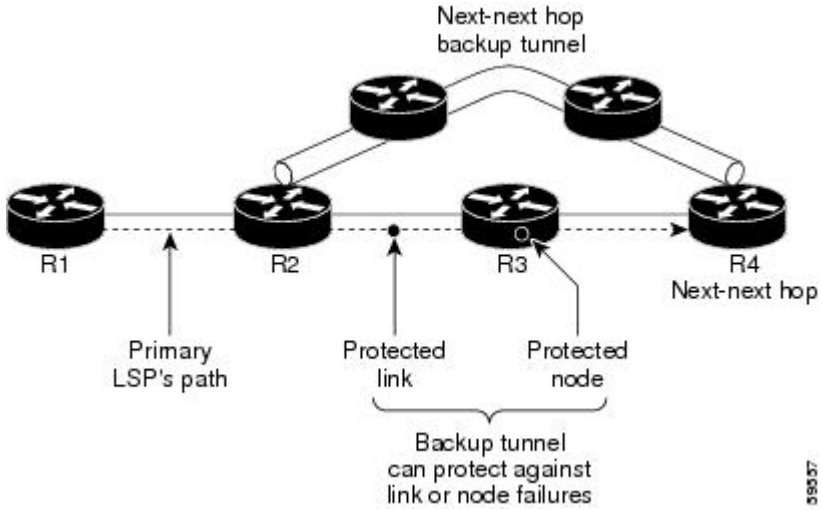


Node Protection

Backup tunnels that bypass next-hop nodes along LSP paths are called NNHOP backup tunnels because they terminate at the node following the next-hop node of the LSPs, thereby bypassing the next-hop node. They protect LSPs by enabling the node upstream of a link or node failure to reroute the LSPs and their traffic around the failure to the next-hop node. NNHOP backup tunnels also provide protection from link failures because they bypass the failed link and the node.

The figure below illustrates an NNHOP backup tunnel.

Figure 2: Next-Next Hop Backup Tunnel



Explicit Paths

Explicit paths are used to create backup autotunnels as follows:

- NHOP excludes the protected link's IP address.
- NNHOP excludes the NHOP router ID.
- The explicit-path name is _auto-tunnel_tunnel*xxx* , where *xxx* matches the dynamically created backup tunnel ID.

- The interface used for the **ip unnumbered** command defaults to Loopback0. You can configure this to use a different interface.

Range for Backup Autotunnels

The tunnel range for backup autotunnels is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 1000 to 1100 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the MPLS TE dynamic tunnel software can use those IDs.

MPLS Traffic Engineering Primary Autotunnels

The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS traffic. The tunnels are created with zero bandwidth. The constraint-based shortest path first (CSPF) is the same as the shortest path first (SPF) when there is zero bandwidth, so the router's choice of the autorouted one-hop primary tunnel is the same as if there were no tunnel. Because it is a one-hop tunnel, the encapsulation is tag-implicit (that is, there is no tag header).

Explicit Paths

Explicit paths are used to create autotunnels as follows:

- The explicit path is dynamically created.
- The explicit path includes the IP address for the interface connected to the next hop.
- The explicit-path name is _auto-tunnel_tunnel*xxx* , where *xxx* matches the dynamically created one-hop tunnel ID.
- Interfaces used for the **ip unnumbered** command default to Loopback0. You can configure this to use a different interface.

Range for Autotunnels

The tunnel range is configurable. By default, the last 100 TE tunnel IDs are used; that is 65,436 to 65,535. Autotunnels detect tunnel IDs that are being used. IDs are allocated starting with the lowest number.

For example, if you configure a tunnel range 100 to 200 and statically configured TE tunnels are in that range, routers do not use those IDs. If those static tunnels are removed, the IDs become available for use by the MPLS TE dynamic tunnel software.

MPLS Traffic Engineering Label-Based Forwarding

Routers receive a packet, determine where it needs to go by examining some fields in the packet, and send it to the appropriate output device. A label is a short, fixed-length identifier that is used to forward packets. A label switching device normally replaces the label in a packet with a new value before forwarding the packet to the next hop. For this reason, the forwarding algorithm is called label swapping. A label switching device,

referred to as an LSR, runs standard IP control protocols (that is, routing protocols, RSVP, and so forth) to determine where to forward packets.

Benefits of MPLS Traffic Engineering Protection

The following sections describe the benefits of MPLS traffic engineering protection:

DeliveryofPacketsDuringaFailure

Backup tunnels that terminate at the NNHOP protect both the downstream link and node. This provides protection for link and node failures.

Multiple Backup Tunnels Protecting the Same Interface

In addition to being required for node protection, the autotunnel primary and backup feature provides the following benefits:

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

Scalability

A backup tunnel can protect multiple LSPs. Furthermore, a backup tunnel can protect multiple interfaces. This is called many-to-one (N:1) protection. N:1 protection has significant scalability advantages over one-to-one (1:1) protection, where a separate backup tunnel must be used for each LSP needing protection.

An example of N:1 protection is that when one backup tunnel protects 5000 LSPs, each router along the backup path maintains one additional tunnel.

An example of 1:1 protection is that when 5000 backup tunnels protect 5000 LSPs, each router along the backup path must maintain state for an additional 5000 tunnels.

RSVP Hello

RSVP Hello allows a router to detect when its neighbor has gone down but its interface to that neighbor is still operational. When Layer 2 link protocols are unable to detect that the neighbor is unreachable, Hellos provide the detection mechanism; this allows the router to switch LSPs onto its backup tunnels and avoid packet loss.

SSO Redundancy Overview

The SSO feature is an incremental step within an overall program to improve the availability of networks constructed with Cisco IOS routers.

SSO is particularly useful at the network edge. It provides protection for network edge devices with dual route processors (RPs) that represent a single point of failure in the network design, and where an outage might result in loss of service for customers.

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The feature establishes one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizes critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Affinity and Link Attributes with Autotunnel Backup

In Cisco IOS Release 15.1(1)S and later releases, you can use affinity and link attributes with the MPLS TE Autotunnel Backup feature to include or exclude links when configuring dynamic backup paths.

For a link, you can configure up to 32 bits of attribute flags, as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet0/0
Router(config-if)# mpls traffic-eng attribute-flags 0x22
```

The attribute flags are compared to the tunnel's affinity bits during selection of the path.

When you enable the auto-tunnel backup feature, you can optionally specify the affinity and mask, as shown in the following example. If you do not specify an affinity and mask, the default for affinity is 0 and for the mask it is 0xFFFF is used. To ignore link affinity, use affinity and mask of 0. See the **mpls traffic-eng auto-tunnel backup config affinity**command for more information.

```
Router> enable
Router# configure terminal
Router(config)# mpls traffic-eng auto-tunnel backup

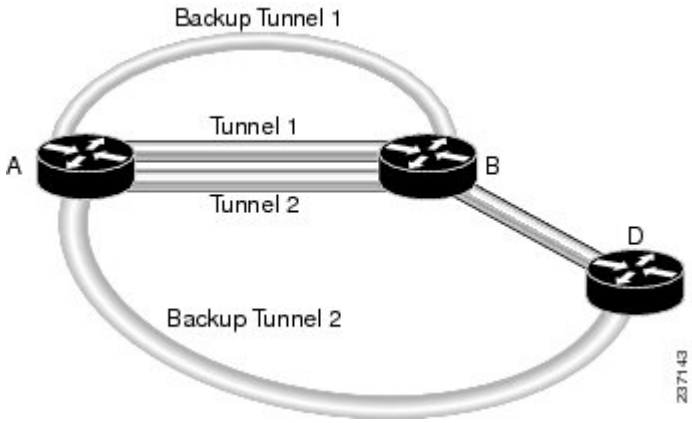
Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x13 mask 0x13
```

The affinity/mask configured by the **mpls traffic-eng auto-tunnel backup config affinity**command is used for all dynamically created backup tunnels. The attribute mask determines which link attributes are relevent. If a bit in the mask is 0, the attribute is irrelevant. If a bit in the mask is 1, the attribute value of a link and the configured affinity of the tunnel for that bit must match.

In the figure below, there are two primary tunnels. One tunnel travels from router A to router B. The other primary tunnel travels from router A to router B and then router D. All the the links are configured with attribute flags 0x22. Both tunnels require fast reroute protection. To automatically create backup tunnels, enable the autotunnel backup feature with the **mpls traffic-eng auto-tunnel backup** command. However, the dynamically created backup tunnels do not come up, because attribute flags are configured on the links. To enable the dynamically created backup tunnels, you must also issue the following command:

Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22

Figure 3: Specifying Link Attributes and Affinity with Autotunnel Backup



How to Configure MPLS Traffic Engineering Autotunnel Primary and Backup

Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs

To establish an MPLS backup autotunnel to protect fast reroutable TE LSPs, perform the following task.

Note Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel backup**
4. **mpls traffic-eng auto-tunnel backup nhop-only**
5. **mpls traffic-eng auto-tunnel backup tunnel-num** [**min** *num*] [**max** *num*]
6. **mpls traffic-eng auto-tunnel backup timers removal unused** *sec*
7. **mpls traffic-eng auto-tunnel backup config unnumbered-interface** *interface*
8. **mpls traffic-eng auto-tunnel backup config affinity** *affinity-value* **mask** *mask-value*]

DETAILED STEPS

Procedure

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng auto-tunnel backup** **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup`	Automatically builds NHOP and NNHOP backup tunnels.
Step 4	**mpls traffic-eng auto-tunnel backup nhop-only** **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup nhop-only`	Enables the creation of dynamic NHOP backup tunnels.
Step 5	**mpls traffic-eng auto-tunnel backup tunnel-num** [**min** *num*] [**max** *num*] **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100`	Configures the range of tunnel interface numbers for backup autotunnels.
Step 6	**mpls traffic-eng auto-tunnel backup timers removal unused** *sec* **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50`	Configures how frequently a timer will scan backup autotunnels and remove tunnels that are not being used. The value for **auto-tunnel backup timers removal unused** cannot be less than 10 mins.
Step 7	**mpls traffic-eng auto-tunnel backup config unnumbered-interface** *interface* **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface ethernet1/0`	Enables IP processing on the specified interface without an explicit address.
Step 8	**mpls traffic-eng auto-tunnel backup config affinity** *affinity-value* **mask** *mask-value*] **Example:** `Router(config)# mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22`	Specifies the affinity values and mask flags. The affinity determines the attribute of the link that the tunnel will use. That is, the attribute for which the tunnel has an affinity. The mask determines which link attribute the router should check. If a bit in the mask is 0, an attribute value of a link or that bit is irrelevant. If a bit in the mask is 1, the attribute values of a link and the required affinity of the tunnel for that bit must match.

Establishing MPLS One-Hop Tunnels to All Neighbors

To establish MPLS one-hop tunnels to all neighbors, perform the following task.

Note Only Steps 1 through 3 are required. If you perform additional steps, you can perform them in any order after Step 3.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng auto-tunnel primary onehop**
4. **mpls traffic-eng auto-tunnel primary tunnel-num** [**min** *num*] [**max***num*]
5. **mpls traffic-eng auto-tunnel primary timers removal rerouted** *sec*
6. **mpls traffic-eng auto-tunnel primary config unnumbered** *interface*
7. **mpls traffic-eng auto-tunnel primary config mpls ip**

DETAILED STEPS

Procedure

	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 auto-tunnel primary onehop** **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary onehop`	Automatically creates primary tunnels to all next hops.
Step 4	**mpls traffic-eng auto-tunnel primary tunnel-num** [**min** *num*] [**max***num*] **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100`	Configures the range of tunnel interface numbers for primary autotunnels.

	Command or Action	Purpose
Step 5	**mpls traffic-eng auto-tunnel primary timers removal rerouted** *sec* **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 400`	Configures how many seconds after a failure primary autotunnels will be removed.
Step 6	**mpls traffic-eng auto-tunnel primary config unnumbered** *interface* **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered ethernet1/0`	Enables IP processing on the specified interface without an explicit address.
Step 7	**mpls traffic-eng auto-tunnel primary config mpls ip** **Example:** `Router(config)# mpls traffic-eng auto-tunnel primary config mpls ip`	Enables LDP on primary autotunnels.

Configuration Examples for MPLS Traffic Engineering-Autotunnel Primary and Backup

Establishing MPLS Backup Autotunnels to Protect Fast Reroutable TE LSPs Example

Note This example does not include the **mpls traffic-eng auto-tunnel backup nhop-only** command because autotunneling would not be able to create any backup tunnels.

To determine if there are any backup tunnels, enter the **show ip rsvp fast-reroute** command. This example shows that there is a static configured primary tunnel and no backup tunnels.

```
Router(config)# show ip rsvp fast-reroute
Primary     Protect   BW         Backup
Tunnel      I/F       BPS:Type   Tunnel:Label  State  Level   Type
------      -------   -------    ------------  ------ -----   ----
R3-PRP_t0   PO3/1     0:G        None          None   None
```

The following command causes autotunnels to automatically configure NHOP and NNHOP backup tunnels:

```
Router(config)# mpls traffic-eng auto-tunnel backup
```

As illustrated in the **show ip interface brief** command output, autotunneling created two backup tunnels that have tunnel IDs 65436 and 65437:

```
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
POS2/0                 10.0.0.14       YES NVRAM  down                  down
POS2/1                 10.0.0.49       YES NVRAM  up                    up
POS2/2                 10.0.0.45       YES NVRAM  up                    up
POS2/3                 10.0.0.57       YES NVRAM  administratively down  down
POS3/0                 10.0.0.18       YES NVRAM  down                  down
POS3/1                 10.0.0.33       YES NVRAM  up                    up
POS3/2                 unassigned      YES NVRAM  administratively down  down
POS3/3                 unassigned      YES NVRAM  administratively down  down
GigabitEthernet4/0     10.0.0.37       YES NVRAM  up                    up
GigabitEthernet4/1     unassigned      YES NVRAM  administratively down  down
GigabitEthernet4/2     unassigned      YES NVRAM  administratively down  down
Loopback0              10.0.3.1        YES NVRAM  up                    up
Tunnel0                10.0.3.1        YES unset  up                    up
Tunnel65436            10.0.3.1        YES unset  up                    up
Tunnel65437            10.0.3.1        YES unset  up                    up
Ethernet0              10.3.38.3       YES NVRAM  up                    up
Ethernet1              unassigned      YES NVRAM  administratively down  down
R3-PRP#
```

The following command prevents autotunneling from creating NNHOP backup tunnels:

```
Router# mpls traffic-eng auto-tunnel backup nhop-only
```

The “Type” field in the following **show ip rsvp fast-reroute** command shows that there is only an NHOP tunnel:

```
Router# show ip rsvp fast-reroute

Primary    Protect  BW Backup
Tunnel     I/F      BPS:Type  Tunnel:Label  State  Level   Type
------     -------  --------  ------------- ------ ------- ----
R3-PRP_t0  PO3/1    0:G       Tu65436:24    Ready  any-unl Nhop
```

The following command changes the minimum and maximum tunnel interface numbers to 1000 and 1100, respectively:

```
Router# mpls traffic-eng auto-tunnel backup tunnel-num min 1000 max 1100
```

You can verify the ID numbers and autotunnel backup range ID by entering the **show ip rsvp fast-reroute** and **show ip interface brief** commands. In this example, only one backup tunnel is protecting the primary tunnel:

```
Router# show ip rsvp fast-reroute

Primary                  Protect BW         Backup
Tunnel                   I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                   ------- --------   ------------- ------ -----   ------
R3-PRP_t0                PO3/1   0:G        Tu1000:24     Ready  any-unl Nhop
Router# show ip interface brief
Interface            IP-Address    OK?  Method  Status                  Protocol
POS2/0               10.0.0.14     YES  NVRAM   down                    down
POS2/1               10.0.0.49     YES  NVRAM   up                      up
POS2/2               10.0.0.45     YES  NVRAM   up                      up
POS2/3               10.0.0.57     YES  NVRAM   administratively down   down
```

```
POS3/0               10.0.0.18     YES  NVRAM   down                    down
POS3/1               10.0.0.33     YES  NVRAM   up                      up
POS3/2               unassigned    YES  NVRAM   administratively down   down
POS3/3               unassigned    YES  NVRAM   administratively down   down
GigabitEthernet4/0   10.0.0.37     YES  NVRAM   up                      up
GigabitEthernet4/1   unassigned    YES  NVRAM   administratively down   down
GigabitEthernet4/2   unassigned    YES  NVRAM   administratively down   down
Loopback0            10.0.3.1      YES  NVRAM   up                      up
Tunnel0              10.0.3.1      YES  unset   up                      up
Tunnel65436          10.0.3.1      YES  unset   up                      up
Ethernet0            10.3.38.3     YES  NVRAM   up                      up
Ethernet1            unassigned    YES  NVRAM   administratively down   down
```

The default tunnel range for autotunnel backup tunnels is 65,436 through 65,535. The following **show ip rsvp fast-reroute** command changes the tunnel range IDs:

```
Router# show ip rsvp fast-reroute

Primary     Protect  BW         Backup
Tunnel       I/F     BPS:Type   Tunnel:Label   State   Level    Type
------      -------  --------   ------------- ------   -----    ------
R3-PRP_t0   PO3/1    0:G        Tu1001:0       Ready   any-unl  N-Nhop
```

The results are shown in the **show ip interface brief** command:

```
Router# show ip interface
Router# show ip interface brief

Interface              UP-Address   OK?  Method  Status                  Protocol
POS2/0                 10.0.0.14    YES  NVRAM   down                    down
POS2/1                 10.0.0.49    YES  NVRAM   up                      up
POS2/2                 10.0.0.45    YES  NVRAM   up                      up
POS2/3                 10.0.0.57    YES  NVRAM   up                      up
POS3/0                 10.0.0.18    YES  NVRAM   up                      up
POS3/1                 10.0.0.33    YES  NVRAM   up                      up
POS3/2                 unassigned   YES  NVRAM   administratively down  down
POS3/3                 unassigned   YES  NVRAM   administratively down  down
Loopback0              10.0.3.1     YES  NVRAM   up                      up
Tunnel0                10.0.3.1     YES  unset   up                      up
Tunnel1000             10.0.3.1     YES  unset   up                      up
Tunnel1001             10.0.3.1     YES  unset   up                      up
Ethernet0              10.3.38.3    YES  NVRAM   up                      up
Ethernet1              unassigned   YES  NVRAM   administratively down  down
```

The following **mpls traffic-eng auto-tunnel backup timers removal unused** command specifies that a timer will scan backup autotunnels every 50 seconds and the timer will remove tunnels that are not being used:

```
Router(config)# mpls traffic-eng auto-tunnel backup timers removal unused 50
```

The following **mpls traffic-eng auto-tunnel backup config unnumbered-interface** command enables IP processing on POS interface 3/1:

```
Router(config)# mpls traffic-eng auto-tunnel backup config unnumbered-interface POS3/1
```

To verify that IP processing is enabled on POS3/1, enter the **show interfaces tunnel** command:

```
Router# show interfaces tunnel 1001
Tunnel1001 is up, line protocol is up
  Hardware is Tunnel
  Interface is unnumbered.  Using address of POS3/1 (10.0.0.33)
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
```

```
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.0, destination 10.0.5.1
  Tunnel protocol/transport Label Switching, sequencing disabled
  Key disabled
  Checksumming of packets disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy: fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The following **mpls traffic-eng auto-tunnel backup config affinity**command specifies affinity and link attributes that help in the calculation of the dynamically created backup tunnel:

Router(config)# **mpls traffic-eng auto-tunnel backup config affinity 0x22 mask 0x22**

To display the affinity and link attributes assigned to a dynamically created backup tunnel, enter the s**how mpls traffic-eng auto-tunnel backup**command:

```
Router# show mpls traffic-eng auto-tunnel backup

State: Enabled
  Tunnel Count: 3 (up:2, down: 1)
  Tunnel ID Range: 65436-65535
  Create Nhop only: Yes
  SRLG: Not configured
  Delete unused tunnels after: 50 Seconds
  Config:
    Unnumbered i/f: Looback0
    Affinity: 0x22/0x22
```

Establishing MPLS One-Hop Tunnels to Neighbors Example

For autotunneling to automatically create primary tunnels to all next hops, you must enter the following command:

```
Router(config)# mpls traffic-eng auto-tunnel primary onehop
```

In this example there are four primary tunnels and no backup tunnels. To verify that configuration, enter the **show ip rsvp fast-reroute** command and the **show ip interface brief** command:

```
Router# show ip rsvp fast-reroute
Primary                  Protect BW         Backup
Tunnel                   I/F     BPS:Type   Tunnel:Label  State  Level   Type
------                   ------- --------   ------------- ------ -----   ------
R3-PRP_t65337            PO2/2   0:G        None          None   None
R3-PRP_t65338            PO3/1   0:G        None          None   None
R3-PRP_t65339            Gi4/0   0:G        None          None   None
R3-PRP_t65336            PO2/1   0:G        None          None   None
Router# show ip interface brief
Interface              IP-Address    OK?  Method Status                Protocol
POS2/0                 10.0.0.14     YES  NVRAM  down                  down
```

```
POS2/1                 10.0.0.49     YES  NVRAM  up                    up
POS2/2                 10.0.0.45     YES  NVRAM  up                    up
POS2/3                 10.0.0.57     YES  NVRAM  administratively down  down
POS3/0                 10.0.0.18     YES  NVRAM  down                  down
POS3/1                 10.0.0.33     YES  NVRAM  up                    up
POS3/2                 unassigned    YES  NVRAM  administratively down  down
POS3/3                 unassigned    YES  NVRAM  administratively down  down
GigabitEthernet4/0     10.0.0.37     YES  NVRAM  up                    up
GigabitEthernet4/1     unassigned    YES  NVRAM  administratively down  down
GigabitEthernet4/2     unassigned    YES  NVRAM  administratively down  down
Loopback0              10.0.3.1      YES  NVRAM  up                    up
Tunnel0                10.0.3.1      YES  unset  administratively down  down
Tunnel65336            10.0.3.1      YES  unset  up                    up
Tunnel65337            10.0.3.1      YES  unset  up                    up
Tunnel65338            10.0.3.1      YES  unset  up                    up
Tunnel65339            10.0.3.1      YES  unset  up                    up
Ethernet0              10.3.38.3     YES  NVRAM  up                    up
Ethernet1              unassigned    YES  NVRAM  administratively down  down
R3-PRP#
```

The default tunnel range for primary autotunnels is 65,336 through 65,435. The following **mpls traffic-eng auto-tunnel primary tunnel-num** command changes the range to 2000 through 2100:

```
Router(config)# mpls traffic-eng auto-tunnel primary tunnel-num min 2000 max 2100
```

The following sample output from the **show ip rsvp fast-reroute** command and the **show ip interface brief** command shows that the tunnel IDs are 2000, 2001, 2002, and 2003:

```
Router# show ip rsvp fast-reroute
Primary                   Protect BW          Backup
Tunnel                    I/F     BPS:Type    Tunnel:Label  State  Level   Type
------                    ------- --------    ------------- ------ -----   ------
R3-PRP_t2001              PO2/2   0:G         None          None   None
R3-PRP_t2002              PO3/1   0:G         None          None   None
R3-PRP_t2003              Gi4/0   0:G         None          None   None
R3-PRP_t2000              PO2/1   0:G         None          None   None
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
POS2/0                 10.0.0.14       YES NVRAM  down                  down
POS2/1                 10.0.0.49       YES NVRAM  up                    up
POS2/2                 10.0.0.45       YES NVRAM  up                    up
POS2/3                 10.0.0.57       YES NVRAM  administratively down down
POS3/0                 10.0.0.18       YES NVRAM  down                  down
POS3/1                 10.0.0.33       YES NVRAM  up                    up
POS3/2                 unassigned      YES NVRAM  administratively down down
POS3/3                 unassigned      YES NVRAM  administratively down down
GigabitEthernet4/0     10.0.0.37       YES NVRAM  up                    up
GigabitEthernet4/1     unassigned      YES NVRAM  administratively down down
GigabitEthernet4/2     unassigned      YES NVRAM  administratively down down
Loopback0              10.0.3.1        YES NVRAM  up                    up
Tunnel0                10.0.3.1        YES unset  administratively down down
Tunnel2000             10.0.3.1        YES unset  up                    up
Tunnel2001             10.0.3.1        YES unset  up                    up
Tunnel2002             10.0.3.1        YES unset  up                    up
Tunnel2003             10.0.3.1        YES unset  up                    up
Ethernet0              10.3.38.3 '     YES NVRAM  up                    up
Ethernet1              unassigned      YES NVRAM  administratively down down
```

The following **mpls traffic-eng auto-tunnel primary timers**command specifies that a timer will scan backup autotunnels every 50 seconds and remove tunnels that are not being used:

```
Router(config)# mpls traffic-eng auto-tunnel primary timers removal rerouted 50
```

The following **mpls traffic-eng auto-tunnel primary config unnumbered** command enables IP processing on POS interface 3/1:

```
Router(config)# mpls traffic-eng auto-tunnel primary config unnumbered POS3/1
```

To specify that autotunneling remove all primary autotunnels and re-create them, enter the following command:

```
Router(config)# clear mpls traffic-eng auto-tunnel primary
```

Additional References

The following sections provide references related to the MPLS Traffic Engineering-Autotunnel Primary and Backup feature.

Additional References

Related Topic	Document Title
Backup tunnels	MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
Link protection	MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection)
MPLS traffic engineering commands	*Cisco IOS Multiprotocol Label Switching Command Reference*
SSO	*Cisco IOS High Availability Configuration Guide*

Standards

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

MIBs

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

RFCs

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

Technical Assistance

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

Feature Information for MPLS Traffic Engineering-Autotunnel Primary and Backup

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

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

Table 1: Feature Information for MPLS Traffic Engineering-Autotunnel Primary and Backup

Feature Name	Releases	Feature Configuration Information
MPLS Traffic Engineering-Autotunnel Primary and Backup	12.0(27)S 12.2(33)SRA 12.2(33)SXH 12.4(20)T 12.2(33)SRE 15.1(1)S Cisco IOS XE Release 2.3	The MPLS Traffic Engineering-Autotunnel Primary and Backup feature enables a router to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels. In Cisco IOS Release 12.0(27)S, this feature was introduced. In Cisco IOS Release 12.2(33)SRA, this feature was integrated. In Cisco IOS Release 12.2(33)SXH, support was added. In Cisco IOS Release 12.4(20)T, this feature was integrated. In Cisco IOS Release 12.2(33)SRE. this feature was integrated. A router with primary one-hop autotunnels and backup autotunnels can be configured with SSO redundancy. In Cisco IOS Release 15.1(1)S, this feature was updated to allow you to specify affinity/mask for dynamically created MPLS TE backup tunnels. In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. The following commands were introduced: **affinity**, **mpls traffic-eng auto-tunnel backup config**, **show mpls traffic-eng auto-tunnel backup**.
MPLS TE - Autotunnel/Automesh SSO Coexistence	15.2(1)T Cisco IOS XE Release 3.5S	In Cisco IOS XE Release 3.5S, this feature was integrated. In Cisco IOS Release 15.2(1)T, this feature was integrated. **Note** Starting with Cisco IOS Release 15.2(2)S and Cisco IOS XE Release 3.6S, the SSO Support for MPLS TE Autotunnel and Automesh feature replaces the MPLS TE - Autotunnel/Automesh SSO Coexistence feature. For more information, see the *MPLS High Availability Configuration Guide* for the new implementation.

Glossary

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

egress router --A router at the edge of the network where packets are leaving.

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

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

interface --A network connection.

IP address --A 32-bit address assigned to hosts using TCP/IP. An IP address belongs to one of five classes (A, B, C, D, or E) and is written as four octets separated by periods (dotted decimal format). Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork information from the IP address.

IP explicit path --A list of IP addresses, each representing a node or link in the explicit path.

LDP --Label Distribution Protocol. A standard protocol between MPLS-enabled routers to negotiate the labels (addresses) used to forward packets.

link --Point-to-point connection between adjacent nodes.

LSP --label switched path. A path that is followed by a labeled packet over several hops, starting at an ingress LSR and ending at an egress LSR.

LSR --label switch router. A Layer 3 router that forwards a packet based on the value of a label encapsulated in the packet.

MPLS --Multiprotocol Label Switching. A method for forwarding packets (frames) through a network. It enables routers at the edge of a network to apply labels to packets. ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

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

penultimate router --The second-to-last router; that is, the router that is immediately before the egress router.

primary tunnel --An MPLS tunnel whose LSP can be fast rerouted if there is a failure.

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

router ID --Something by which a router originating a packet can be uniquely distinguished from all other routers. For example, an IP address from one of the router's interfaces.

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

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