RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

This document describes support for link protection also referred as next-hop (NHOP) protection using the backup Segment-Routing Traffic Engineering (SR-TE) autotunnel. It protect the links over which the RSVP Traffic Engineering (RSVP-TE) tunnel traverses.

Feature Information for RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Table 1: Feature Information for RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

Feature Name	Releases	Feature Information
RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel	Cisco IOS XE Amsterdam 17.3.2	This feature provides support for link protection also referred as next-hop (NHOP) protection using the backup Segment-Routing Traffic Engineering (SR-TE) autotunnel. It protect the links over which the RSVP Traffic Engineering (RSVP-TE) tunnel traverses. The following commands were introduced by this feature: **ip explicit-path name path1 enable**, **show mpls traffic-eng tunnels tunnel 65436**, **show ip explicit-paths**, **show mpls traffic-eng tunnels tunnel 65436 | show Segment-Routing Path Info**, **show mpls traffic-eng fast-reroute database**, **show ip rsvp fast-reroute sh mpls traffic-eng auto-tunnel backup**.

Prerequisites for RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

Before enabling SR-TE backup autotunnel, ensure that the following technologies are configured in your setup:

- IS-IS Network Point to Point Interfaces
- Segment Routing

Additionally, prior knowledge of the following technologies are required:

- MPLS Traffic-Engineering
- RSVP Traffic-Engineering
- Fast reroute

Restrictions for RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

- SR-TE backup autotunnel cannot be used for bandwidth protection.
- SR-TE backup autotunnel can only be used as a backup for RSVP-TE tunnel protection.

Information About RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

Benefits of RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

With increased complexity in the network, scalability becomes a challenge due to maintenance of RSVP-TE tunnels with complex signaling as well as high overhead on routers within the network. Backup autotunnel feature can help reduce the complexity in a Segment Routing (SR) network. Autotunnel backup feature has the following benefits:

- Backup tunnels are built automatically hence eliminating the need for users to pre-configure each backup tunnel and then assign the backup tunnel to the protected interface.
- With the backup tunnels configured, area of protection gets expanded. Fast reroute (FRR) neither protects IP traffic nor LDP labels that do not use TE tunnel.
- Backup SR-TE autotunnel allows additional means of migration to SR network without disrupting the existing traffic passing through RSVP-TE tunnels.

Backup AutoTunnel

Backup autotunnels on a router helps to build dynamic backup tunnels whenever required. This prevents creating of static SR-TE tunnels.

To protect a label-switched path (LSP) in the absence of static SR-TE tunnels, you need 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 protection attribute.
- Detection of changed Record Route Object (RRO).

If there is no backup tunnel protecting the interface used by the LSP, the LSP remained unprotected. Some of the reasons why a backup tunnel may not be available are:

- Static backup tunnels are not configured.
- Static backup tunnels are configured, but may not be able to protect the LSP because there is not enough bandwidth available, or the tunnel protects a different pool, or the tunnel is not available.

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

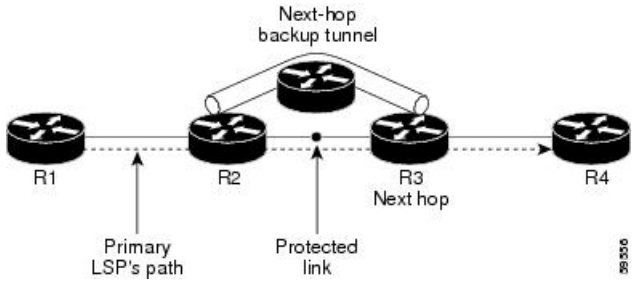
- NHOP—Protects against link failure.
- NNHOP—Protects against node failure.

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

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 NHOP backup tunnels because they terminate at the LSP's next hop beyond the point of failure.

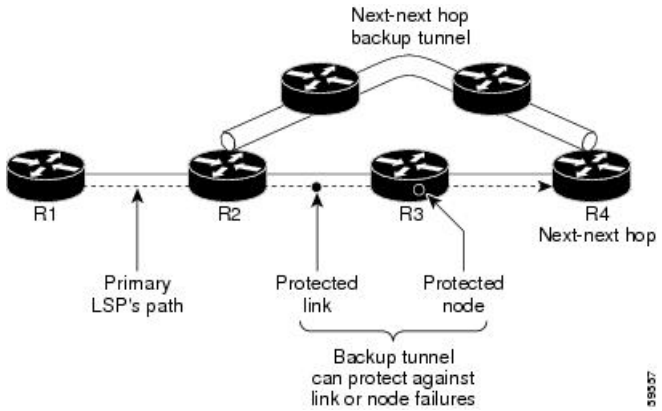
Figure 1: Next-Hop Backup Tunnel



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.

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.

Range for Backup AutoTunnels

You can configure the tunnel range for backup autotunnels. By default, the last 100 TE tunnel IDs are used, which is 65,436 to 65,535. Autotunnels detect tunnel IDs that are alloted starting with the lowest number.

For example, if you configure a tunnel within the range of 1000 to 1100. And statically configured TE tunnel also falls in the same range then routers do not use those IDs. If those static tunnels are removed, the MPLS-TE dynamic tunnel software can use those IDs.

How to Configure RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

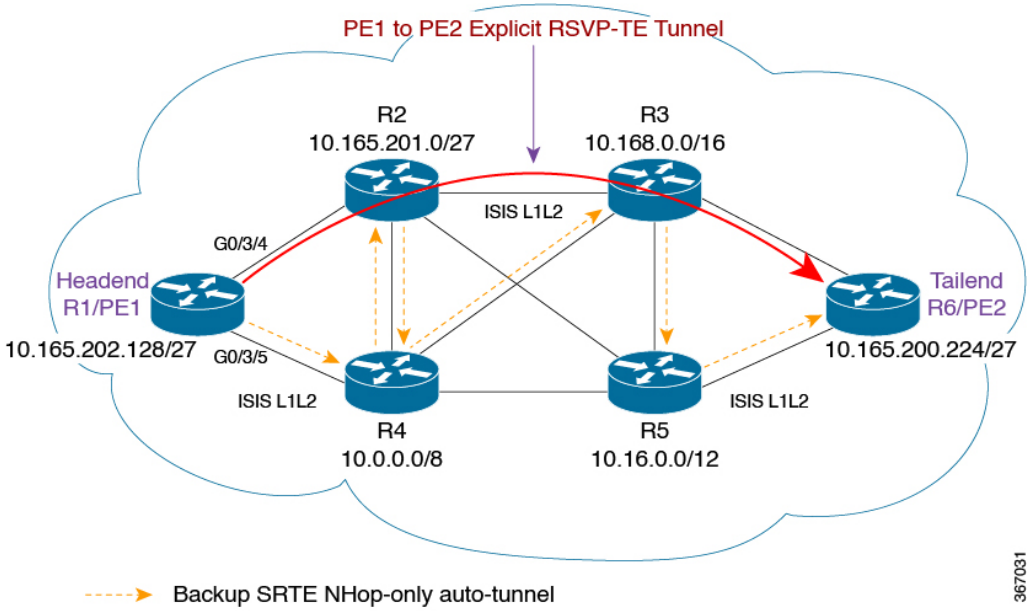
Configuring Explicit Path for Point-to-Point Network Type

For SR-TE autotunnel backup feature to work interfaces have to be point-to-point network type.

```
interface Loopback0
 ip address 10.51.1.1 255.255.255.255
 ip router isis 1
end
!
interface GigabitEthernet0/2/0
 ip address 10.102.6.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
!
interface GigabitEthernet0/2/4
 ip address 10.104.1.1 255.255.255.0
 ip router isis 1
 negotiation auto
 mpls traffic-eng tunnels
 isis network point-to-point
 ip rsvp bandwidth
end
```

Configuring Explicit RSVP-TE Tunnel With FRR

Figure 3: Explicit RSVP-TE Tunnel



1. Configure explicit path from R1/PE1 to R6/PE2 that traverses through the routers R2 and R3.

```
ip explicit-path name path1 enable
 index 1 next-address 10.165.202.128
 index 2 next-address 10.165.201.0
 index 3 next-address 10.168.0.0
 index 4 next-address 10.165.200.224
```

2. Configure explicit RSVP-TE tunnel.

```
interface Tunnel1
 ip unnumbered Loopback0
 tunnel mode mpls traffic-eng
 tunnel destination 10.165.200.224
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng path-option 10 explicit name path1
 tunnel mpls traffic-eng record-route
end
```

3. Configure the primary RSVP-TE Tunnel 1 with FRR to activate the protection process.

```
interface tunnel 1
 tunnel mpls traffic-eng fast-reroute
```

4. Configure the global command to enable link protection using SR-TE autotunnel.

```
mpls traffic-eng auto-tunnel backup segment-routing nhop-only
```

Note This command needs to be available in all the nodes that require link protection.

The Primary RSVP-TE tunnel need to be protected that gets initialized from headend R1/PE1 to destination R6/PE2 and traversing through next node R2 and so on. In this case, R1/PE1 is the Point of Local Repair (PLR) and R2 is the Mid-Point (MP). With link protection, the SR-TE Backup AutoTunnel provides protection to the link from R1/PE1 to R2 by traversing through the path R1/PE1 -> R4 and R4 -> R2, hence converging back to the MP.

Verifying RSVP-TE Protection using Segment Routing Traffic Engineering AutoTunnel

Use the **show interfaces Tunnel** command to verify if SR-TE AutoTunnel is generated and up.

```
Device#show interfaces Tunnel65436
Tunnel65436 is up, line protocol is up
```

Use the **show mpls traffic-eng tunnels** command to verify if the backup AutoTunnel is a SR-TE Tunnel.

```
Device#show mpls traffic-eng tunnels tunnel 65436
Name: R1_t65436 (Tunnel65436) Destination: 10.165.201.0
 Status:
  Admin: up Oper: up Path: valid Signalling: connected
  path option 1, (SEGMENT-ROUTING) type explicit __dynamic_tunnel65436 (Basis for
Setup, path weight 20)
```

Use the **show ip explicit-paths** command to verify if the SR-TE Backup Tunnel is using a secondary path to reach the node.

```
Device#show ip explicit-paths
PATH __dynamic_tunnel65436 (strict source route, path complete, generation 49, status
non-configured)
1: exclude-address 10.102.5.1
```

Use the **show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info** command to verify if the backup tunnel is going through the path R1/PE1 to R4 and finally to destination R2 which is the mid-point.

```
Device#show mpls traffic-eng tunnels tunnel 65436 | s Segment-Routing Path Info
Segment-Routing Path Info (isis level-1)
 Segment0[Link]: 10.104.1.1 - 10.104.1.2, Label: 19
 Segment1[Link]: 10.104.6.2 - 10.104.6.1, Label: 18
```

Use the **show mpls traffic-eng auto-tunnel backup** command to verify if the auto-tunnel backup state is correct.

```
Device#show mpls traffic-eng auto-tunnel backup
State: Enabled
 Auto backup tunnels: 1 (up: 1, down: 0)
 Tunnel ID Range: 65436 - 65535
```

```
 Create Nhop Only: Yes
 Check for deletion of unused tunnels every: 3600 Sec
 SRLG: Not configured

Config:
 unnumbered-interface: Loopback0
  Affinity/Mask: 0x0/0xFFFF
```

Use the **show mpls traffic-eng fast-reroute database** command to verify if the primary link through which the RSVP-TE LSP is traversing is protected.

```
Device#show mpls traffic-eng fast-reroute database
P2P Headend FRR information:
Protected tunnel In-label Out intf/label FRR intf/label Status
-------------------------- -------- -------------- -------------- ------
Tunnel1 Tun hd Gi0/3/4:30 Tu65436:30 ready


Device#show ip rsvp fast-reroute
P2P Protect BW Backup
Protected LSP I/F BPS:Type Tunnel:Label State Level Type
------------- ------- -------- ------------- ------ ----- ------
R1_t1 Gi0/3/4 0:G Tu65436:28 Ready any-unl Nhop
```