

SSO Support for MPLS TE Autotunnel and Automesh

The SSO Support for MPLS TE Autotunnel and Automesh feature provides full stateful switchover (SSO), Cisco nonstop forwarding (NSF), and In Service Software Upgrade (ISSU) support for autotunnel primary and backup TE tunnels feature and for autotunnel mesh group TE tunnels feature.

The NSF with SSO provides continuous packet forwarding even during a network processor hardware or software failure. In a redundant system, the secondary processor recovers control plane service during a critical failure in the primary processor. SSO synchronizes the network state information between the primary and the secondary processor.

Note For brevity in this document, the Autotunnel Primary and Backup feature is called Autotunnel. The Autotunnel Mesh Groups feature is called Automesh.

- Prerequisites for SSO Support for MPLS TE Autotunnel and Automesh, on page 1
- Restrictions for SSO Support for MPLS TE Autotunnel and Automesh, on page 2
- Information About SSO Support for MPLS TE Autotunnel and Automesh, on page 2
- Additional References, on page 3
- Feature Information for SSO Support for MPLS TE Autotunnel and Automesh, on page 3
- Glossary, on page 4

Prerequisites for SSO Support for MPLS TE Autotunnel and Automesh

- The MPLS TE RSVP Graceful Restart feature must be enabled on the stateful switchover (SSO) device and its neighbor devices.
- NSF must be configured on the IGP that is configured for TE. You must specify either the **nsf cisco** or the **nsf ietf** router configuration command or the recovery of TE tunnels might fail.
- The MPLS TE Autotunnel feature must be configured.
- The MPLS TE Automesh feature must be configured.

Note The SSO Support for MPLS TE Autotunnel and Automesh feature obsoletes the MPLS TE Autotunnel and SSO Coexistence feature available with the MPLS TE Autotunnel feature and the MPLS TE Automesh feature.

Restrictions for SSO Support for MPLS TE Autotunnel and Automesh

- The SSO Support for MPLS TE Autotunnel and Automesh feature is supported only on hardware platforms with dual Route Processors (RPs) that support SSO and Cisco NSF.
- SSO and Fast Reroute (FRR) double failure cases are not supported.
- To keep the Autotunnel and Automesh configurations synchronized between the active and standby RPs, you can no longer modify an existing Autotunnel or Automesh interface by using the **interface tunnel** command. This action is prohibited by the software.
- You can no longer use the following commands as a way for disabling the Autotunnel or the Automesh feature:
  - **clear mpls traffic-eng auto-tunnel primary**
  - **clear mpls traffic-eng auto-tunnel backup**
  - **clear mpls traffic-eng auto-tunnel mesh**

  Instead, use the **no** form of these commands:
  - **no mpls traffic-eng auto-tunnel primary onehop**
  - **no mpls traffic-eng auto-tunnel backup**
  - **no mpls traffic-eng auto-tunnel mesh**

Information About SSO Support for MPLS TE Autotunnel and Automesh

Overview of SSO Support for MPLS TE Autotunnel and Automesh

With the SSO Support for MPLS TE Autotunnel and Automesh feature, once you enable the device for the Autotunnel feature or for the Automesh feature by using the **mpls traffic-eng auto-tunnel primary onehop**, **mpls traffic-eng auto-tunnel backup**, or the **mpls traffic-eng auto-tunnel mesh** commands, the device starts creating the specified type of autotunnel on both the active and standby RPs. No additional configuration is needed to implement the SSO Support for MPLS TE Autotunnel and Automesh feature.

When the **no** form of these commands is executed, the SSO feature is disabled on both the active and the standby RPs.

The Autotunnel feature enables a device to dynamically build backup tunnels and to dynamically create one-hop primary tunnels on all interfaces that have been configured with MPLS TE tunnels.

The Automesh feature allows a network administrator to configure TE label switched paths (LSPs). In a network topology where edge label switch routers (LSRs) are connected by core LSRs, the Automesh feature automatically constructs a mesh of TE LSPs among the provider edge (PE) devices.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	*Master Commands List, All Releases*
MPLS traffic engineering commands	*Multiprotocol Label Switching Command Reference*
MPLS traffic engineering—Autotunnel Mesh Groups feature	*MPLS Traffic Engineering Path Calculation and Setup Configuration Guide*
MPLS traffic engineering—Autotunnel Primary and Backup feature	*MPLS Traffic Engineering Path Link and Node Protection Configuration Guide*

Technical Assistance

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

Feature Information for SSO Support for MPLS TE Autotunnel and Automesh

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 SSO Support for MPLS TE Autotunnel and Automesh

Feature Name	Releases	Feature Information
SSO Support for MPLS TE Autotunnel and Automesh	15.2(2)S Cisco IOS XE Release 3.6S	The SSO Support for MPLS TE Autotunnel and Automesh feature provides full stateful switchover (SSO), Cisco nonstop forwarding (NSF), and In Service Software Upgrade (ISSU) support for the autotunnel primary and backup TE tunnels and for the autotunnel mesh group TE tunnels. The following commands were introduced or modified: **clear mpls traffic-eng auto-tunnel backup tunnel**, **clear mpls traffic-eng auto-tunnel mesh tunnel**, **clear mpls traffic-eng auto-tunnel primary tunnel**, **debug mpls traffic-eng auto-tunnel backup**, **debug mpls traffic-eng auto-tunnel primary**, **debug mpls traffic-eng ha sso**, **mpls traffic-eng auto-tunnel backup**, **mpls traffic-eng auto-tunnel mesh**, **mpls traffic-eng auto-tunnel primary onehop**, **show ip rsvp high-availability counters**, **show ip rsvp high-availability database**, **show ip rsvp high-availability database summary**, **show ip rsvp high-availability summary**, **show mpls traffic-eng auto-tunnel primary**.

Glossary

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

Fast Reroute—Fast Reroute (FRR) is a mechanism for protecting MPLS traffic engineering 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 devices attempt to establish end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over backup tunnels that bypass failed links or nodes.

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

ISSU—In Service Software Upgrade. Software upgrade without service interruption.

LSP—label switched path. A path that a labeled packet follows over several hops, starting at an ingress LSR and ending at an egress LSR.

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

mesh group—A set of label switch routers (LSRs) that are members of a full or partial network of traffic engineering label switched paths (LSPs).

MPLS—Multiprotocol Label Switching. A switching method that forwards IP traffic using a label. This label instructs the devices in the network where to forward the packets based on preestablished IP routing information.

NSF—nonstop forwarding. The ability of a device to continue to forward traffic to a device that may be recovering from a failure. Also, the ability of a device recovering from a failure to continue to correctly forward traffic sent to it by a peer.

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

SSO—stateful switchover. SSO refers to the implementation of Cisco software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. Along with NSF, SSO makes an RP failure undetectable to the network.

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

tunnel—A secure communication path between two peers. A traffic engineering tunnel is a label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than a normal Layer 3 device.