# MPLS Traffic Engineering Path Calculation and Setup Configuration Guide, Cisco IOS XE Release 2

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

# CONTENTS

# MPLS Traffic Engineering and Enhancements

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what previously could be achieved only by overlaying a Layer 3 network on a Layer 2 network.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering and Enhancements

Your network must support the following Cisco IOS XE features before you enable MPLS traffic engineering:

- Multiprotocol Label Switching
- IP Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

# Restrictions for MPLS Traffic Engineering and Enhancements

- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/ instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.
- MPLS traffic engineering does not support ATM MPLS-controlled subinterfaces.
- The MPLS traffic engineering feature does not support routing and signaling of LSPs over unnumbered IP links. Therefore, do not configure the feature over those links.

# Information About MPLS Traffic Engineering and Enhancements



## Introduction to MPLS Traffic Engineering and Enhancements

Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what now can be achieved only by overlaying a Layer 3 network on a Layer 2 network.

Traffic engineering is essential for service provider and Internet service provider (ISP) backbones. Such backbones must support a high use of transmission capacity, and the networks must be very resilient so that they can withstand link or node failures.

MPLS traffic engineering provides an integrated approach to traffic engineering. With MPLS, traffic engineering capabilities are integrated into Layer 3, which optimizes the routing of IP traffic, given the constraints imposed by backbone capacity and topology.

MPLS traffic engineering supports the following functionality:

- Enhances standard Interior Gateway Protocols (IGPs), such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows.
- Transports traffic flows across a network using MPLS forwarding.

- Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources available in the network.
- Employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS traffic engineering, the traffic flow has bandwidth requirements, media requirements, a priority that is compared to the priority of other flows, and so forth.
- Recovers from link or node failures by adapting to the new constraints presented by the changed topology.
- Transports packets using MPLS forwarding crossing a multihop label switched path (LSP).
- Uses the routing and signaling capability of LSPs across a backbone topology that
    - Understands the backbone topology and available resources
    - Accounts for link bandwidth and for the size of the traffic flow when determining routes for LSPs across the backbone
    - Has a dynamic adaptation mechanism that enables the backbone to be resilient to failures, even if several primary paths are precalculated off-line
    - Includes enhancements to the IGP (IS-IS or OSPF) shortest path first (SPF) calculations to automatically calculate what traffic should be sent over what LSPs.

# Benefits of MPLS Traffic Engineering

WAN connections are an expensive item in an ISP budget. Traffic engineering enables ISPs to route network traffic to offer the best service to their users in terms of throughput and delay. By making the service provider more efficient, traffic engineering reduces the cost of the network.

Currently, some ISPs base their services on an overlay model. In th e overlay model, transmission facilities are managed by Layer 2 switching. The routers see only a fully meshed virtual topology, making most destinations appear one hop away. If you use the explicit Layer 2 transit layer, you can precisely control how traffic uses available bandwidth. However, the overlay model has numerous disadvantages. MPLS traffic engineering achieves the traffic engineering benefits of the overlay model without running a separate network, and without needing a nonscalable, full mesh of router interconnects.

# How MPLS Traffic Engineering Works

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone by using RSVP. The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth.

Available resources are flooded by means of extensions to a link-state based IGP.

Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint-based routing). The IGP automatically routes the traffic onto these LSPs. Typically, a packet crossing the MPLS traffic engineering backbone travels on a single LSP that connects the ingress point to the egress point.

MPLS traffic engineering is built on the following Cisco IOS XE mechanisms:

- IP tunnel interfaces

From a Layer 2 standpoint, an MPLS tunnel interface represents the head of an LSP. It is configured with a set of resource requirements, such as bandwidth and media requirements, and priority.

From a Layer 3 standpoint, an LSP tunnel interface is the headend of a unidirectional virtual link to the tunnel destination.

- MPLS traffic engineering path calculation module

This calculation module operates at the LSP head. The module determines a path to use for an LSP. The path calculation uses a link-state database containing flooded topology and resource information.

- RSVP with traffic engineering extensions

RSVP operates at each LSP hop and is used to signal and maintain LSPs based on the calculated path.

- MPLS traffic engineering link management module

This module operates at each LSP hop, does link call admission on the RSVP signaling messages, and bookkeeping of topology and resource information to be flooded.

- Link-state IGP (IS-IS or OSPF--each with traffic engineering extensions)

These IGPs are used to globally flood topology and resource information from the link management module.

- Enhancements to the SPF calculation used by the link-state IGP (IS-IS or OSPF)

The IGP automatically routes traffic onto the appropriate LSP tunnel based on tunnel destination. Static routes can also be used to direct traffic onto LSP tunnels.

- Label switching forwarding

This forwarding mechanism provides routers with a Layer 2-like ability to direct traffic across multiple hops of the LSP established by RSVP signaling.

One approach to engineering a backbone is to define a mesh of tunnels from every ingress device to every egress device. The MPLS traffic engineering path calculation and signaling modules determine the path taken by the LSPs for these tunnels, subject to resource availability and the dynamic state of the network. The IGP, operating at an ingress device, determines which traffic should go to which egress device, and steers that traffic into the tunnel from ingress to egress.

A flow from an ingress device to an egress device might be so large that it cannot fit over a single link, so it cannot be carried by a single tunnel. In this case, multiple tunnels between a given ingress and egress can be configured, and the flow is load-shared among them.

# Mapping Traffic into Tunnels

This section describes how traffic is mapped into tunnels; that is, how conventional hop-by-hop link-state routing protocols interact with MPLS traffic engineering capabilities. In particular, this section describes how the shortest path first (SPF) algorithm, sometimes called a Dijkstra algorithm, has been enhanced so that a link-state IGP can automatically forward traffic over tunnels that MPLS traffic engineering establishes.

Link-state protocols, like integrated IS-IS or OSPF, use an SPF algorithm to compute a shortest path tree from the headend node to all nodes in the network. Routing tables are derived from this shortest path tree. The routing tables contain ordered sets of destination and first-hop information. If a router does normal hop-by-hop routing, the first hop is over a physical interface attached to the router.

New traffic engineering algorithms calculate explicit routes to one or more nodes in the network. The originating router views these explicit routes as logical interfaces. In the context of this document, these explicit routes are represented by LSPs and referred to as traffic engineering tunnels (TE tunnels).

The following sections describe how link-state IGPs can use these shortcuts, and how they can install routes in the routing table that point to these TE tunnels. These tunnels use explicit routes, and the path taken by a TE tunnel is controlled by the router that is the headend of the tunnel. In the absence of errors, TE tunnels are guaranteed not to loop, but routers must agree on how to use the TE tunnels. Otherwise, traffic might loop through two or more tunnels. See the following sections:


- Enhancement to the SPF Computation, page 5
- Special Cases and Exceptions for SPF Calculations, page 5
- Additional Enhancements to SPF Computation Using Configured Tunnel Metrics, page 6


## Enhancement to the SPF Computation

During each step of the SPF computation, a router discovers the path to one node in the network.

- If that node is directly connected to the calculating router, the first-hop information is derived from the adjacency database.
- If the node is not directly connected to the calculating router, the node inherits the first-hop information from the parent(s) of that node. Each node has one or more parents, and each node is the parent of zero or more downstream nodes.

For traffic engineering purposes, each router maintains a list of all TE tunnels that originate at this headend router. For each of those TE tunnels, the router at the tailend is known to the head-end router.

During the SPF computation, the TENT (tentative) list stores paths that are possibly the best paths and the PATH list stores paths that are definitely the best paths. When it is determined that a path is the best possible path, the node is moved from TENT to PATH. PATH is thus the set of nodes for which the best path from the computing router has been found. Each PATH entry consists of ID, path cost, and forwarding direction.

The router must determine the first-hop information. There are several ways to do this:

- Examine the list of tailend routers directly reachable by a TE tunnel. If there is a TE tunnel to this node, use the TE tunnel as the first hop.
- If there is no TE tunnel and the node is directly connected, use the first-hop information from the adjacency database.
- If the node is not directly connected and is not directly reachable by a TE tunnel, copy the first-hop information from the parent node(s) to the new node.

As a result of this computation, traffic to nodes that are the tail end of TE tunnels flows over the TE tunnels. Traffic to nodes that are downstream of the tail-end nodes also flows over the TE tunnels. If there is more than one TE tunnel to different intermediate nodes on the path to destination node X, traffic flows over the TE tunnel whose tail-end node is closest to node X.

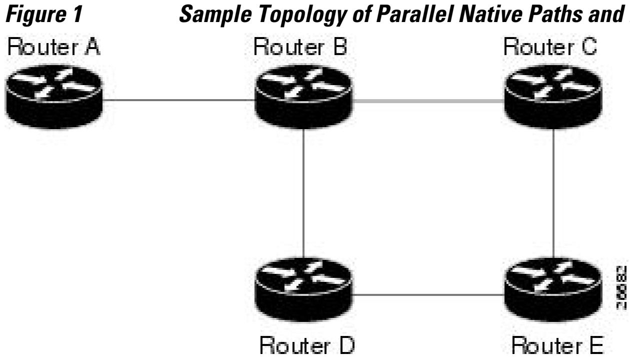
## Special Cases and Exceptions for SPF Calculations

The SPF algorithm finds equal-cost parallel paths to destinations. The enhancement previously described does not change this. Traffic can be forwarded over any of the following:

- One or more native IP paths
- One or more traffic engineering tunnels
- A combination of native IP paths and traffic engineering tunnels

A special situation occurs in the topology shown in the figure below.

***Figure 1 Sample Topology of Parallel Native Paths and Paths Over TE Tunnels***



If parallel native IP paths and paths over TE tunnels are available, the following implementations allow you to force traffic to flow over TE tunnels only or only over native IP paths. Assume that all links have the same cost and that a TE tunnel is set up from Router A to Router D.

- When the SPF calculation puts Router C on the TENT list, it realizes that Router C is not directly connected. It uses the first-hop information from the parent, which is Router B.
- When the SPF calculation on Router A puts Router D on the TENT list, it realizes that Router D is the tail end of a TE tunnel. Thus Router A installs a route to Router D by the TE tunnel, and not by Router B.
- When Router A puts Router E on the TENT list, it realizes that Router E is not directly connected, and that Router E is not the tail end of a TE tunnel. Therefore Router A copies the first-hop information from the parents (Router C and Router D) to the first-hop information of Router E.

Traffic to Router E now load balances over

- The native IP path by Router A to Router B to Router C
- The TE tunnel Router A to Router D

## Additional Enhancements to SPF Computation Using Configured Tunnel Metrics

When traffic engineering tunnels install an IGP route in a Router Information Base (RIB) as next hops, the distance or metric of the route must be calculated. Normally, you could make the metric the same as the IGP metric over native IP paths as if the TE tunnels did not exist. For example, Router A can reach Router C with the shortest distance of 20. X is a route advertised in IGP by Router C. Route X is installed in Router A's RIB with the metric of 20. When a TE tunnel from Router A to Router C comes up, by default the route is installed with a metric of 20, but the next-hop information for X is changed.

Although the same metric scheme can work well in other situations, for some applications it is useful to change the TE tunnel metric (for instance, when there are equal cost paths through TE tunnel and native IP links). You can adjust TE tunnel metrics to force the traffic to prefer the TE tunnel, to prefer the native IP paths, or to load share among them.

Suppose that multiple TE tunnels go to the same destination or different destinations. TE tunnel metrics can force the traffic to prefer some TE tunnels over others, regardless of IGP distances to those destinations.

Setting metrics on TE tunnels does not affect the basic SPF algorithm. It affects only two questions:

1. Is the TE tunnel installed as one of the next hops to the destination routers?
2. What is the metric value of the routes being installed into the RIB?

You can modify the metrics for determining the first-hop information in one of the following ways:

- If the metric of the TE tunnel to the tailend routers is higher than the metric for the other TE tunnels or native hop-by-hop IGP paths, this tunnel is not installed as the next hop.
- If the metric of the TE tunnel is equal to the metric of either other TE tunnels or native hop-by-hop IGP paths, this tunnel is added to the existing next hops.
- If the metric of the TE tunnel is lower than the metric of other TE tunnels or native hop-by-hop IGP paths, this tunnel replaces them as the only next hop.

In each of the above cases, the IGP assigns metrics to routes associated with those tailend routers and their downstream routers.

The SPF computation is loop free because the traffic through the TE tunnels is basically source routed. The end result of TE tunnel metric adjustment is the control of traffic loadsharing. If there is only one way to reach the destination through a single TE tunnel, then no matter what metric is assigned, the traffic has only one way to go.

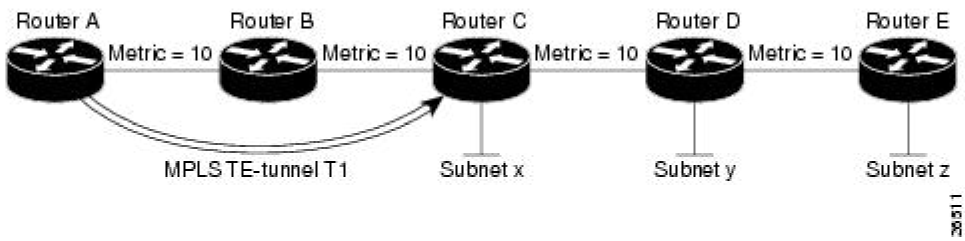
You can represent the TE tunnel metric in two different ways: (1) as an absolute (or fixed) metric or (2) as a relative (or floating) metric.

If you use an absolute metric, the routes assigned with the metric are fixed. This metric is used not only for the routes sourced on the TE tunnel tailend router, but also for each route downstream of this tailend router that uses this TE tunnel as one of its next hops.

For example, if you have TE tunnels to two core routers in a remote point of presence (POP), and one of them has an absolute metric of 1, all traffic going to that POP traverses this low-metric TE tunnel.

If you use a relative metric, the actual assigned metric value of routes is based on the IGP metric. This relative metric can be positive or negative, and is bounded by minimum and maximum allowed metric values. For example, assume the topology shown in the figure below.

*Figure 2 Topology That Has No Traffic Engineering Tunnel*




If there is no TE tunnel, Router A installs routes x, y, and z and assigns metrics 20, 30, and 40 respectively. Suppose that Router A has a TE tunnel T1 to Router C. If the relative metric -5 is used on tunnel T1, the routers x, y, and z have the installed metrics of 15, 25, and 35. If an absolute metric of 5 is used on tunnel T1, routes x, y and z have the same metric 5 installed in the RIB for Router A. The assigning of no metric on the TE tunnel is a special case, a relative metric scheme where the metric is 0.

# Transition of an IS-IS Network to a New Technology

IS-IS, as specified in RFC 1142, includes extensions for MPLS traffic engineering and for other purposes. Running MPLS traffic engineering over IS-IS or taking advantage of these other extensions requires transitioning an IS-IS network to this new technology. This section describes these extensions and discusses two ways to migrate an existing IS-IS network from the standard ISO 10589 protocol towards the version of IS-IS specified in RFC 1142.Running MPLS traffic engineering over an existing IS-IS network requires a transition to the version of IS-IS specified in RFC 1142. However, running MPLS traffic engineering over OSPF does **not** require any similar network transition.

# Extensions for the IS-IS Routing Protocol

Extensions for the IS-IS routing protocol serve the following purposes:

- Remove the 6-bit limit on link metrics.
- Allow interarea IP routes.
- Enable IS-IS to carry different kinds of information for traffic engineering. In the future, more extensions might be needed.

To serve these purposes, two new TLVs (type, length, and value objects) have been defined:

- TLV 22 describes links (or rather adjacencies). It serves the same purpose as the “IS neighbor option” in ISO 10589 (TLV 2).

- TLV 135 describes reachable IP prefixes. It is similar to the IP Neighbor options from RFC 1195 (TLVs 128 and 130).

**Note** For the purpose of briefness, these two new TLVs, 22 and 135, are referred to as “new-style TLVs.” TLVs 2, 128, and 130 are referred to as “old-style TLVs.”

Both new TLVs have a fixed length part, followed by optional sub-TLVs. The metric space in these new TLVs has been enhanced from 6 bits to 24 or 32 bits. The sub-TLVs allow you to add new properties to links and prefixes. Traffic engineering is the first technology to use this ability to add new properties to a link.

# Problems with Old and New TLVs in Theory and in Practice

Link-state routing protocols compute loop-free routes. This is guaranteed because all routers calculate their routing tables based on the same information from the link-state database (LSPDB).

There is a problem when some routers look at old-style TLVs and some routers look at new-style TLVs because the routers can base their SPF calculations on different information. This can cause routing loops.

The easiest way to migrate from old-style TLVs towards new-style TLVs would be to introduce a “flag day.” A flag day means that you reconfigure all routers during a short period of time, during which service is interrupted. If the implementation of a flag day is not acceptable, a network administrator needs to find a viable solution for modern existing networks.

Network administrators have the following problems related to TLVs:

- They need to run an IS-IS network where some routers are advertising and using the new-style TLVs and, at the same time, other routers are capable only of advertising and using old-style TLVs.
- They need to test new traffic engineering software in existing networks on a limited number of routers. They cannot upgrade all their routers in their production networks or in their test networks before they start testing.

The new extensions allow a network administrator to use old-style TLVs in one area, and new-style TLVs in another area. However, this is not a solution for administrators who need or want to run their network in one single area.

The following sections describe two solutions to the network administrator’s problems.

# First Solution for Transitioning an IS-IS Network to a New Technology

When you migrate from old-style TLVs towards new-style TLVs, you can advertise the same information twice--once in old-style TLVs and once in new-style TLVs. This ensures that all routers can understand what is advertised.

There are three disadvantages to using that approach:

- Size of the LSPs--During the transition, the LSPs grow to about twice their original size. This might be a problem in networks where the LSPDB is large. An LSPDB might be large because
    - There are many routers, and thus LSPs.
    - There are many neighbors or IP prefixes per router. A router that advertises lots of information causes the LSPs to be fragmented.
- Unpredictable results--In a large network, this solution can produce unpredictable results. A large network in transition pushes the limits regarding LSP flooding and SPF scaling. During the transition

    - You can expect some extra network instability. At this time, you especially do not want to test how far you can push an implementation.
    - Traffic engineering extensions might cause LSPs to be reflooded frequently.
- Ambiguity--If a router encounters different information in the old-style TLVs and the new-style TLVs, it may not be clear what the router should do.

These problems can be largely solved easily by using

- All information in old-style and new-style TLVs in an LSP
- The adjacency with the lowest link metric if an adjacency is advertised more than once

The main benefit to advertising the same information twice is that network administrators can use new-style TLVs before all routers in the network can understand them.

## Transition Actions During the First Solution

When transitioning from using IS-IS with old-style TLVs to new-style TLVs, you can perform the following actions:

- If all routers run old software, advertise and use only old-style TLVs.
- Upgrade some routers to newer software.
- Configure some routers with new software to advertise both old-style and new-style TLVs. They accept both styles of TLVs. Configure other routers (with old software) to continue advertising and using only old-style TLVs.
- Test traffic engineering in parts of your network; however, new-style TLVs cannot be used yet.
- If the whole network needs to migrate, upgrade and configure all remaining routers to advertise and accept both styles of TLVs.
- Configure all routers to advertise and accept only new-style TLVs.
- Configure metrics larger than 63.

For more information about how to perform these actions, see the TLV Configuration Commands section.

## Second Solution for Transitioning an IS-IS Network to a New Technology

Routers advertise only one style of TLVs at the same time, but can understand both types of TLVs during migration. There are two main benefits to this approach:

- LSPs stay approximately the same size during migration.
- There is no ambiguity when the same information is advertised twice inside one LSP.

This method is useful when you are transitioning the whole network (or a whole area) to use wider metrics (that is, you want a router running IS-IS to generate and accept only new-style TLVs). For more information, see the **metric-style wide**command.

The disadvantage is that all routers must understand the new-style TLVs before any router can start advertising new-style TLVs. It does not help the second problem, where network administrators want to use the new-style TLVs for traffic engineering, while some routers are capable of understanding only old-style TLVs.

## Transition Actions During the Second Solution

If you use the second solution, you can perform the following actions:

- If all routers run old software, advertise and use only old-style TLVs.

- Upgrade all routers to newer software.
- Configure all routers one-by-one to advertise old-style TLVs, but to accept both styles of TLVs.
- Configure all routers one-by-one to advertise new-style TLVs, but to accept both styles of TLVs.
- Configure all routers one-by-one to advertise and to accept only new-style TLVs.
- Configure metrics larger than 63.

## TLV Configuration Commands

Cisco IOS XE has a **router isis**command-line interface (CLI) command called **metric-style**. Once the router is in IS-IS configuration mode, you have the option to choose the following:

- **metric-style narrow** --Enables the router to generate and accept only old-style TLVs
- **metric-style transition** --Enables the router to generate and accept both old-style and new-style TLVs
- **metric-style wide** --Enables the router to generate and accept only new-style TLVs

You can use either of the following two transition schemes when you use the **metric-style**command to configure:

- Narrow to transition to wide
- Narrow to narrow transition to wide transition to wide

## Implementation in Cisco IOS XE Software

Cisco IOS XE implements both transitions solution. Network administrators can choose the solution that suits them best. For test networks, the first solution is best (go to the First Solution for Transitioning an IS-IS Network to a New Technology, page 8). For a full transition, both solutions can be used. The first solution requires fewer steps and less configuration. You would use the second solution for the largest networks where a risk of doubling the LSPDB during transition exists, (go to the Second Solution for Transitioning an IS-IS Network to a New Technology, page 9).

# How to Configure MPLS Traffic Engineering and Enhancements

# Configuring a Device to Support Tunnels

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef**
4. **mpls traffic-eng tunnels**
5. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip cef**<br><br>**Example:**<br><br>`Router(config)# ip cef` | Enables standard Cisco Express Forwarding operation. |
| **Step 4** | **mpls traffic-eng tunnels**<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng tunnels` | Enables the MPLS traffic engineering tunnel feature on a device. |
| **Step 5** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits to privileged EXEC mode. |

# Configuring an Interface to Support RSVP-Based Tunnel Signaling and IGP Flooding

**Note** You must enable the tunnel feature on interfaces that you want to support MPLS traffic engineering.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **mpls traffic-eng tunnels**
5. **ip rsvp bandwidth** *bandwidth*
6. **exit**
7. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br>`Router(config)# interface serial 1/0/0` | Configures an interface type and enters interface configuration mode. |
| Step 4 | **mpls traffic-eng tunnels**<br><br>**Example:**<br>`Router(config-if)# mpls traffic-eng tunnels` | Enables MPLS traffic engineering tunnels on an interface. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **ip rsvp bandwidth** *bandwidth*<br><br>**Example:**<br><br>`Router(config-if)# ip rsvp bandwidth 1000` | Enables RSVP for IP on an interface and specifies the amount of bandwidth that will be reserved. |
| **Step 6** | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 7** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the following steps.

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/ instance.

### SUMMARY STEPS

1. Router(config)# **router isis**
2. Router(config-router)# **mpls traffic-eng level-1**
3. Router(config-router)# **mpls traffic-eng level-2**
4. Router(config-router)# **mpls traffic-eng router-id loopback 0**
5. Router(config-router)# **metric-style wide**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **router isis** | Enables IS-IS routing and specifies an IS-IS process for IP. The router is placed in configuration mode. |
| **Step 2** | Router(config-router)# **mpls traffic-eng level-1** | Turns on MPLS traffic engineering for IS-IS level 1. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | Router(config-router)# **mpls traffic-eng level-2** | Turns on MPLS traffic engineering for IS-IS level 2. |
| **Step 4** | Router(config-router)# **mpls traffic-eng router-id loopback 0** | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0. |
| **Step 5** | Router(config-router)# **metric-style wide** | Configures a router to generate and accept only new-style type, length, value objects (TLVs). |

• Configuring OSPF for MPLS Traffic Engineering, page 14

# Configuring OSPF for MPLS Traffic Engineering

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **mpls traffic-eng area** *number*
5. **mpls traffic-eng router-id loopback0**
6. **exit**
7. **exit**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **router ospf** *process-id*<br><br>**Example:**<br><br>`Router(config)# router ospf 200` | Configures an OSPF routing process for IP and enters router configuration mode.<br><br>• The *process-id* is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process. |
| Step 4 | **mpls traffic-eng area** *number*<br><br>**Example:**<br><br>`Router(config-router)# mpls traffic-eng area 0` | Turns on MPLS traffic engineering for the indicated OSPF area. |
| Step 5 | **mpls traffic-eng router-id loopback0**<br><br>**Example:**<br><br>`Router(config-router)# mpls traffic-eng router-id loopback0` | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0. |
| Step 6 | **exit**<br><br>**Example:**<br><br>`Router(config-router)# exit` | Exits to global configuration mode. |
| Step 7 | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits to privileged EXEC mode. |

# Configuring an MPLS Traffic Engineering Tunnel

This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **tunnel destination** *ip-address*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** *bandwidth*
8. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | **identifier** *path-number*}} [**lockdown**]
9. **exit**
10. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br><br>`Router(config)# interface Tunnel0` | Configures an interface type and enters interface configuration mode.<br><br>• The *number*argument is the number of the tunnel. |
| Step 4 | **ip unnumbered** *type number*<br><br>**Example:**<br><br>`Router(config-if)# ip unnumbered loopback0` | Enables IP processing on an interface without assigning an explicit IP address to the interface.<br><br>• The *type* and *number* arguments name the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.<br>• An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **tunnel destination** *ip-address*<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 192.168.4.4` | Specifies the destination for a tunnel interface.<br><br>• The *ip-address* argument must be the MPLS traffic engineering router ID of the destination device. |
| Step 6 | **tunnel mode mpls traffic-eng**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | Sets the tunnel encapsulation mode to MPLS traffic engineering. |
| Step 7 | **tunnel mpls traffic-eng bandwidth** *bandwidth*<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 250` | Configures the bandwidth for the MPLS traffic engineering tunnel.<br><br>• The *bandwidth* argument is a number in kilobits per second that is set aside for the MPLS traffic engineering tunnel. Range is from 1 to 4294967295.<br><br>**Note** If automatic bandwidth is configured for the tunnel, use the **tunnel mpls traffic-eng bandwidth** command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism. |
| Step 8 | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name** *path-name* \| **identifier** *path-number*}} [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit identifier 321` | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.<br><br>• The *number* argument is the preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000.<br>• The **dynamic** keyword indicates that the path of the label switched path (LSP) is dynamically calculated.<br>• The **explicit** keyword indicates that the path of the LSP is an IP explicit path.<br>• The **name** *path-name* keyword and argument are the path name of the IP explicit path that the tunnel uses with this option.<br>• The **identifier** *path-number*keyword and argument pair names the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.<br>• The **lockdown** keyword specifies that The LSP cannot be reoptimized.<br><br>**Note** A dynamic path is used if an explicit path is currently unavailable. |
| Step 9 | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

• DEFAULT STEPS, page 18

## DEFAULT STEPS

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **tunnel destination** *ip-address*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** *bandwidth*
8. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name*} | **identifier** *path-number*} [**lockdown**]
9. **exit**
10. **exit**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br><br>`Router(config)# interface tunnel10` | Configures an interface type and enters interface configuration mode. |
| Step 4 | **ip unnumbered** *type number*<br><br>**Example:**<br><br>`Router(config-if)# ip unnumbered loopback 0` | Gives the tunnel interface an IP address.<br><br>• An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |
| Step 5 | **tunnel destination** *ip-address*<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 10.20.1.1` | Specifies the destination for a tunnel.<br><br>• The *ip-address* keyword is the IP address of the host destination expressed in dotted decimal notation. |
| Step 6 | **tunnel mode mpls traffic-eng**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | Sets the tunnel encapsulation mode to MPLS traffic engineering. |
| Step 7 | **tunnel mpls traffic-eng bandwidth** *bandwidth*<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 1000` | Configures the bandwidth for the MPLS traffic engineering tunnel. |
| Step 8 | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name** *path-name*} \| **identifier** *path-number*} [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit identifier 1` | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.<br><br>• A dynamic path is used if an explicit path is currently unavailable. |
| Step 9 | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring an MPLS Traffic Engineering Tunnel that an IGP Can Use

This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.


- DEFAULT STEPS, page 20


## DEFAULT STEPS

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng autoroute announce**
5. **exit**
6. **exit**

### DETAILED STEPS

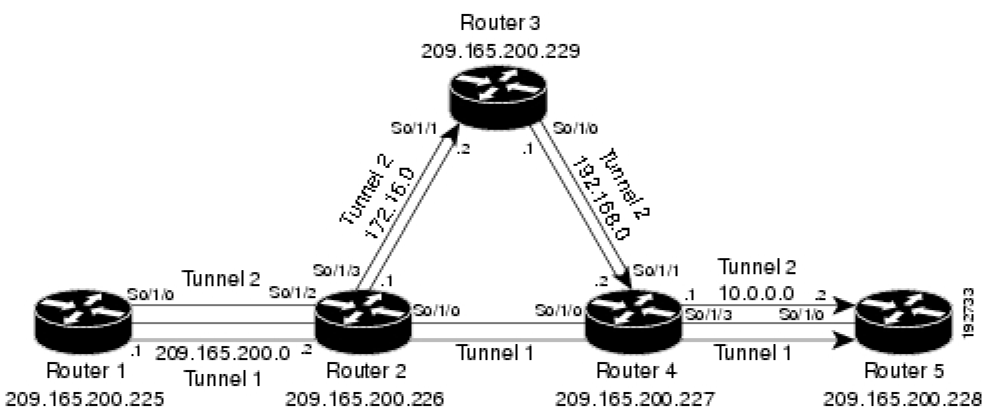
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface tunnel** *number*<br><br>**Example:**<br><br>`Router(config)# interface tunnel1` | Configures an interface type and enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **tunnel mpls traffic-eng autoroute announce**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng autoroute announce` | Causes the IGP to use the tunnel in its enhanced SPF calculation. |
| **Step 5** | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuration Examples for MPLS Traffic Engineering and Enhancements

The figure below illustrates a sample MPLS topology. This example specifies point-to-point outgoing interfaces. The next sections contain sample configuration commands you enter to implement MPLS traffic engineering and the basic tunnel configuration shown in Figure 3.

***Figure 3 Sample MPLS Traffic Engineering Tunnel Configuration***




- Example Configuring MPLS Traffic Engineering Using IS-IS, page 22
- Example Configuring MPLS Traffic Engineering Using OSPF, page 22

- Example Configuring an MPLS Traffic Engineering Tunnel, page 23
- Example Configuring Enhanced SPF Routing over a Tunnel, page 24


# Example Configuring MPLS Traffic Engineering Using IS-IS

This example lists the commands you enter to configure MPLS traffic engineering with IS-IS routing enabled (see the figure above).

**Note** You must enter the following commands on every router in the traffic-engineered portion of your network.


- Router 1--MPLS Traffic Engineering Configuration, page 22
- Router 1--IS-IS Configuration, page 22


## Router 1--MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 10.0.0.0 255.255.255.254
ip router isis
interface s1/0/0
ip address 209.165.200.1 255.255.0.0
ip router isis
mpls traffic-eng tunnels
ip rsvp bandwidth 1000
```

## Router 1--IS-IS Configuration

To enable IS-IS routing, enter the following commands:

```
router isis
network 47.0000.0011.0011.00
is-type level-1
metric-style wide
mpls traffic-eng router-id loopback0
mpls traffic-eng level-1
```

# Example Configuring MPLS Traffic Engineering Using OSPF

This example lists the commands you enter to configure MPLS traffic engineering with OSPF routing enabled (see the figure above).

**Note** You must enter the following commands on every router in the traffic-engineered portion of your network.


- Router 1--MPLS Traffic Engineering Configuration, page 23
- Router 1--OSPF Configuration, page 23

### Router 1--MPLS Traffic Engineering Configuration

To configure MPLS traffic engineering, enter the following commands:

```
ip cef
mpls traffic-eng tunnels
interface loopback 0
ip address 209.165.200.225 255.255.255.255
interface s1/0/0
ip address 209.165.200.1 255.255.0.0
mpls traffic-eng tunnels
  ip rsvp bandwidth 1000
```

### Router 1--OSPF Configuration

To enable OSPF, enter the following commands:

```
router ospf 0
network 209.165.200.0.0.0.255.255 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

## Example Configuring an MPLS Traffic Engineering Tunnel

This example shows you how to configure a dynamic path tunnel and an explicit path in the tunnel. Before you configure MPLS traffic engineering tunnels, you must enter the appropriate global and interface commands on the specified router (in this case, Router 1).


- Router 1--Dynamic Path Tunnel Configuration, page 23
- Router 1--Dynamic Path Tunnel Verification, page 23
- Router 1--Explicit Path Configuration, page 23
- Router 1--Explicit Path Tunnel Configuration, page 24
- Router 1--Explicit Path Tunnel Verification, page 24


### Router 1--Dynamic Path Tunnel Configuration

In this section, a tunnel is configured to use a dynamic path.

```
interface tunnel1
  ip unnumbered loopback 0
  tunnel destination 209.165.200.228
  tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
  tunnel mpls traffic-eng path-option 1 dynamic
```

### Router 1--Dynamic Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up.

```
show mpls traffic-eng tunnels
show ip interface tunnel1
```

### Router 1--Explicit Path Configuration

In this section, an explicit path is configured.

```
ip explicit-path identifier 1
 next-address 209.165.200.1
 next-address 172.16.0.1
 next-address 192.168.0.1
 next-address 10.0.0.1
```

## Router 1--Explicit Path Tunnel Configuration

In this section, a tunnel is configured to use an explicit path.

```
interface tunnel2
  ip unnumbered loopback 0
  tunnel destination 209.165.200.228
  tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 100
  tunnel mpls traffic-eng priority 1 1
  tunnel mpls traffic-eng path-option 1 explicit identifier 1
```

## Router 1--Explicit Path Tunnel Verification

This section includes the commands you use to verify that the tunnel is up.

```
show mpls traffic-eng tunnels
show ip interface tunnel2
```

# Example Configuring Enhanced SPF Routing over a Tunnel

This section includes the commands that cause the tunnel to be considered by the IGP's enhanced SPF calculation, which installs routes over the tunnel for appropriate network prefixes.

- Router 1--IGP Enhanced SPF Consideration Configuration, page 24
- Router 1--Route and Traffic Verification, page 24

## Router 1--IGP Enhanced SPF Consideration Configuration

In this section, you specify that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation.

```
interface tunnel1
tunnel mpls traffic-eng autoroute announce
```

## Router 1--Route and Traffic Verification

This section includes the commands you use to verify that the tunnel is up and that the traffic is routed through the tunnel.

```
show traffic-eng tunnels tunnel1 brief
show ip route 209.165.200.228
show mpls traffic-eng autoroute
ping 209.165.200.228
show interface tunnel1 accounting
show interface s1/0/0 accounting
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Configuring Integrated IS-IS | *Cisco IOS XE IP Routing Protocols Configuration Guide* |
| IS-IS commands | *Cisco IOS IP Routing Protocols Command Reference* |
| Configuring OSPF | *Cisco IOS XE IP Routing Protocols Configuration Guide* |
| OSPF command | *Cisco IOS IP Routing Protocols Command Reference* |
| Configuring Multiprotocol Label Switching | *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* |
| MPLS TE commands | *Cisco IOS Multiprotocol Label Switching Command Reference* |
| RSVP commands | *Cisco IOS Quality of Service Solutions Command Reference* |

### Standards

| Standard | Title |
|---|---|
| None | -- |

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| 1142 | *IS-IS* |

| RFC | Title |
|---|---|
| 1195 | *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments* |
| 2205 | *Resource ReSerVation Protocol (RSVP)* |
| 2328 | *OSPF Version 2* |
| 2370 | *The OSPF Opaque LSA Option* |

### Technical Assistance

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

# Feature Information for MPLS Traffic Engineering and Enhancements

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 and Enhancements*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering and Enhancements | Cisco IOS XE Release 2.3 | Multiprotocol Label Switching (MPLS) traffic engineering software enables an MPLS backbone to replicate and expand upon the traffic engineering capabilities of Layer 2 ATM and Frame Relay networks. MPLS is an integration of Layer 2 and Layer 3 technologies. By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. Thus, you can offer in a one-tier network what previously could be achieved only by overlaying a Layer 3 network on a Layer 2 network.<br>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |
| | | The following commands were introduced or modified:**ip explicit-path**, **metric-style narrow**, **metric-style transition**, **metric-style wide**, **mpls traffic-eng**, **mpls traffic-eng area**, **mpls traffic-eng router-id**, **mpls traffic-eng tunnels**(configuration), **mpls traffic-eng tunnels**(interface), **show mpls traffic-eng autoroute**, **show mpls traffic-eng tunnels**, **tunnel mode mpls traffic-eng**, **tunnel mode mpls traffic-eng autoroute announce**, **tunnel mpls traffic-eng bandwidth**, **tunnel mpls traffic-eng path-option**, **tunnel mpls traffic-eng priority.** |

# Glossary

**affinity** --An MPLS traffic engineering tunnel's requirements on the attributes of the links it will cross. The tunnel's affinity bits and affinity mask bits must match the attribute bits of the various links carrying the tunnel.

**call admission precedence** --An MPLS traffic engineering tunnel with a higher priority will, if necessary, preempt an MPLS traffic engineering tunnel with a lower priority. Tunnels that are harder to route are expected to have a higher priority and to be able to preempt tunnels that are easier to route. The assumption is that lower-priority tunnels will be able to find another path.

**constraint-based routing** --Procedures and protocols that determine a route across a backbone take into account resource requirements and resource availability instead of simply using the shortest path.

**flow** --A traffic load entering the backbone at one point--point of presence (POP)--and leaving it from another, that must be traffic engineered across the backbone. The traffic load is carried across one or more LSP tunnels running from the entry POP to the exit POP.

**headend** --The upstream, transmit end of a tunnel.

**IGP** --Interior Gateway Protocol. The Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include IGRP, OSPF, and RIP.

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

**IS-IS** --Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol that calls for intermediate system (IS) routers to exchange routing information based on a single metric to determine network topology.

**label switched path (LSP)** --A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through label switching mechanisms. A label switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**label switched path (LSP) tunnel** --A configured connection between two routers, in which label switching is used to carry the packets.

**label switching router (LSR)** --A Layer 3 router that forwards packets based on the value of a label encapsulated in the packets.

**LCAC** --Link-level (per hop) call admission control.

**LSA** --Link-state advertisement. Flooded packet used by OSPF that contains information about neighbors and path costs. In IS-IS, receiving routers use LSAs to maintain their routing tables.

LSP--See label switched path.

**OSPF protocol** --Open Shortest Path First. A link state routing protocol used for routing IP.

reoptimization--Reevaluation of the most suitable path for a tunnel to use, given the specified constraints.

**RSVP** --Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

**tailend** --The downstream, receive end of a tunnel.

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

# MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels

The MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels feature enables the user to control the metric used in path calculation for traffic engineering (TE) tunnels on a per-tunnel basis. Certain tunnels are used to carry voice traffic, which requires low delay, and other tunnels are used to carry data. A TE link metric can be used to represent link delay and configure tunnels that carry voice traffic for path calculation and configure tunnels that carry data to use the Interior Gateway Protocol (IGP) metric for path calculation.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels

Before you configure tunnel path calculation metrics, your network must support the following Cisco IOS XE features:

- Multiprotocol Label Switching (MPLS) traffic engineering tunnels
- IP Cisco Express Forwarding
- Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS)

# Restrictions for MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels

- Unless explicitly configured, the TE link metric for a given link is the IGP link metric. When the TE link metric is used to represent a link property that is different from cost/distance, you must configure every network link that can be used for TE tunnels with a TE link metric that represents that property by using the **mpls traffic-eng administrative-weight** command. Failure to do so might cause tunnels to use unexpected paths.
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/ instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

# Information About MPLS Traffic Engineering--RSVP Hello State Timer

## Overview

When MPLS TE is configured in a network, the IGP floods two metrics for every link: the normal IGP (OSPF or IS-IS) link metric and a TE link metric. The IGP uses the IGP link metric in the normal way to compute routes for destination networks.

You can specify that the path calculation for a given tunnel be based on either of the following:

- IGP link metrics.
- TE link metrics, which you can configure so that they represent the needs of a particular application. For example, the TE link metrics can be configured to represent link transmission delay.

## Benefits

When TE tunnels are used to carry two types of traffic, the Configurable Path Calculation Metric for Tunnels feature allows you to tailor tunnel path selection to the requirements of each type of traffic.

For example, suppose certain tunnels are to carry voice traffic (which requires low delay) and other tunnels are to carry data. In this situation, you can use the TE link metric to represent link delay and do the following:

- Configure tunnels that carry voice to use the TE link metric set to represent link delay for path calculation.
- Configure tunnels that carry data to use the IGP metric for path calculation.

# How to Configure MPLS Traffic Engineering--Verbatim Path Support



## Configuring a Platform to Support Traffic Engineering Tunnels

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip cef distributed**
4. **mpls traffic-eng tunnels**
5. **exit**

**DETAILED STEPS**

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip cef distributed**<br><br>**Example:**<br><br>`Router(config)# ip cef distributed` | Enables distributed Cisco Express Forwarding operation. |
| Step 4 | **mpls traffic-eng tunnels**<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng tunnels` | Enables the MPLS traffic engineering tunnel feature on a device. |
| Step 5 | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the following steps.

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

### SUMMARY STEPS

1. Router(config)# **router isis**
2. Router(config-router)# **mpls traffic-eng level-1**
3. Router(config-router)# **mpls traffic-eng level-2**
4. Router(config-router)# **mpls traffic-eng router-id loopback 0**
5. Router(config-router)# **metric-style wide**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Router(config)# **router isis** | Enables IS-IS routing and specifies an IS-IS process for IP. The router is placed in configuration mode. |
| **Step 2** | Router(config-router)# **mpls traffic-eng level-1** | Turns on MPLS traffic engineering for IS-IS level 1. |
| **Step 3** | Router(config-router)# **mpls traffic-eng level-2** | Turns on MPLS traffic engineering for IS-IS level 2. |
| **Step 4** | Router(config-router)# **mpls traffic-eng router-id loopback 0** | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0. |
| **Step 5** | Router(config-router)# **metric-style wide** | Configures a router to generate and accept only new-style type, length, value objects (TLVs). |

• Configuring OSPF for MPLS Traffic Engineering, page 14

## Configuring OSPF for MPLS Traffic Engineering

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/ instance.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router ospf** *process-id*
4. **mpls traffic-eng area** *number*
5. **mpls traffic-eng router-id loopback0**
6. **exit**
7. **exit**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **router ospf** *process-id*<br><br>**Example:**<br><br>`Router(config)# router ospf 200` | Configures an OSPF routing process for IP and enters router configuration mode.<br><br>• The *process-id* is an internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. Assign a unique value for each OSPF routing process. |
| Step 4 | **mpls traffic-eng area** *number*<br><br>**Example:**<br><br>`Router(config-router)# mpls traffic-eng area 0` | Turns on MPLS traffic engineering for the indicated OSPF area. |
| Step 5 | **mpls traffic-eng router-id loopback0**<br><br>**Example:**<br><br>`Router(config-router)# mpls traffic-eng router-id loopback0` | Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0. |
| Step 6 | **exit**<br><br>**Example:**<br><br>`Router(config-router)# exit` | Exits to global configuration mode. |
| Step 7 | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits to privileged EXEC mode. |

# Configuring Traffic Engineering Link Metrics

Unless explicitly configured, the TE link metric is the IGP link metric.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **mpls traffic-eng administrative-weight** *weight*
5. **exit**
6. **exit**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br><br>`Router(config)# interface pos2/0/0` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface to be configured.<br>• The *slot* argument is the chassis slot number. Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.<br>• The **/** *subslot* keyword and argument pair is the secondary slot number on a SIP where a SPA is installed. The slash (/) is required.<br><br>Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.<br>• The **/** *port* keyword and argument pair is the port or interface number. The slash (/) is required.<br><br>Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide<br>• The **.** *subinterface-number*keyword and argument pair is the subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs. |
| Step 4 | **mpls traffic-eng administrative-weight** *weight*<br><br>**Example:**<br><br>`Router(config-if)# mpls traffic-eng administrative-weight 20` | Overrides the IGP administrative weight (cost) of the link.<br>• The *weight* argument is the cost of the link. |
| Step 5 | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| Step 6 | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring an MPLS Traffic Engineering Tunnel

This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered** *type number*
5. **tunnel destination** *ip-address*
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** *bandwidth*
8. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | **identifier** *path-number*}} [**lockdown**]
9. **exit**
10. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br><br>`Router(config)# interface Tunnel0` | Configures an interface type and enters interface configuration mode.<br><br>• The *number*argument is the number of the tunnel. |
| Step 4 | **ip unnumbered** *type number*<br><br>**Example:**<br><br>`Router(config-if)# ip unnumbered loopback0` | Enables IP processing on an interface without assigning an explicit IP address to the interface.<br><br>• The *type* and *number* arguments name the type and number of another interface on which the router has an assigned IP address. It cannot be another unnumbered interface.<br>• An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **tunnel destination** *ip-address*<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 192.168.4.4` | Specifies the destination for a tunnel interface.<br><br>• The *ip-address* argument must be the MPLS traffic engineering router ID of the destination device. |
| Step 6 | **tunnel mode mpls traffic-eng**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | Sets the tunnel encapsulation mode to MPLS traffic engineering. |
| Step 7 | **tunnel mpls traffic-eng bandwidth** *bandwidth*<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 250` | Configures the bandwidth for the MPLS traffic engineering tunnel.<br><br>• The *bandwidth* argument is a number in kilobits per second that is set aside for the MPLS traffic engineering tunnel. Range is from 1 to 4294967295.<br><br>**Note** If automatic bandwidth is configured for the tunnel, use the **tunnel mpls traffic-eng bandwidth** command to configure the initial tunnel bandwidth, which is adjusted by the autobandwidth mechanism. |
| Step 8 | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name** *path-name* \| **identifier** *path-number*}} [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 10 explicit identifier 321` | Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database.<br><br>• The *number* argument is the preference for this path option. When you configure multiple path options, lower numbered options are preferred. Valid values are from 1 to 1000.<br>• The **dynamic** keyword indicates that the path of the label switched path (LSP) is dynamically calculated.<br>• The **explicit** keyword indicates that the path of the LSP is an IP explicit path.<br>• The **name** *path-name* keyword and argument are the path name of the IP explicit path that the tunnel uses with this option.<br>• The **identifier** *path-number*keyword and argument pair names the path number of the IP explicit path that the tunnel uses with this option. The range is from 1 to 65535.<br>• The **lockdown** keyword specifies that The LSP cannot be reoptimized.<br><br>**Note** A dynamic path is used if an explicit path is currently unavailable. |
| Step 9 | **exit**<br><br>**Example:**<br><br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 10** | **exit**<br><br>**Example:**<br><br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

• DEFAULT STEPS, page 18

# Configuring the Metric Type for Tunnel Path Calculation

Unless explicitly configured, the TE link metric type is used for tunnel path calculation. Two commands are provided for controlling the metric type to be used: an interface configuration command that specifies the metric type to be used for a particular TE tunnel and a global configuration command that specifies the metric type to be used for TE tunnels for which a metric type has not been specified by the interface configuration command.

**Note** If you do not enter either of the path selection metrics commands, the traffic engineering (TE) metric is used.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng path-selection metric** {**igp** | **te**}
5. **exit**
6. **mpls traffic-eng path-selection metric** {**igp** | **te**}
7. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface tunnel** *number*<br><br>**Example:**<br>`Router(config)# interface Tunnel0` | Configures an interface type and enters interface configuration mode.<br>• The *number*argument is the number of the tunnel. |
| **Step 4** | **tunnel mpls traffic-eng path-selection metric** {**igp** \| **te**}<br><br>**Example:**<br>`Router(config-if)# tunnel mpls traffic-eng path-selection metric igp` | Specifies the metric type to use for path calculation for a tunnel.<br>• The **igp** keyword specifies the use of the Interior Gateway Protocol (IGP) metric.<br>• The **te** keyword specifies the use of the traffic engineering (TE) metric. This is the default. |
| **Step 5** | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| **Step 6** | **mpls traffic-eng path-selection metric** {**igp** \| **te**}<br><br>**Example:**<br>`Router(config)# mpls traffic-eng path-selection metric igp` | Specifies the metric type to use if a metric type was not explicitly configured for a given tunnel.<br>• The **igp** keyword specifies the use of the Interior Gateway Protocol (IGP) metric.<br>• The **te** keyword specifies the use of the traffic engineering (TE) metric. This is the default. |
| **Step 7** | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Verifying the Tunnel Path Metric Configuration

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng topolog** y
3. **show mpls traffic-eng tunnels**
4. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng topolog** y

Use the **show mpls traffic-eng topology** command, which displays TE and IGP metrics for each link, to verify that link metrics have been correctly configured for a network. For example:

**Example:**

```
Router# show mpls traffic-eng topology
My_System_id: 1440.0000.0044.00 (isis  level-1)
IGP Id: 0090.0000.0009.00, MPLS TE Id:192.168.9.9 Router Node  (isis  level-1)
      link[0 ]:Nbr IGP Id: 0090.0000.0009.03, gen:7
          frag_id 0, Intf Address:10.0.0.99
          TE metric:100, IGP metric:48, attribute_flags:0x0     !!Note TE and IGP metrics
          physical_bw: 10000 (kbps), max_reservable_bw_global: 0 (kbps)
          max_reservable_bw_sub: 0 (kbps)
.
.
.
      link[1 ]:Nbr IGP Id: 0055.0000.0055.00, gen:7
          frag_id 0, Intf Address:10.205.0.9, Nbr Intf Address:10.205.0.55
          TE metric:120, IGP metric:10, attribute_flags:0x0     !!Note TE and IGP metrics
          physical_bw: 155000 (kbps), max_reservable_bw_global: 500000 (kbps)
          max_reservable_bw_sub: 0 (kbps)
.
.
.
```

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

Use the **show mpls traffic-eng tunnels** command, which displays the link metric used for tunnel path calculation, to verify that the desired link metrics are being used for each tunnel. For example:

**Example:**

```
Router# show mpls traffic-eng tunnels
Name: te3640-17-c_t221              (Tunnel22) Destination: 192.168.100.22
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
```

```
    path option 1, type dynamic (Basis for Setup, path weight 10)
  Config Parameters:
    Bandwidth: 400 kps (Global)    Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: IGP                                          !!Note metric type
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 0   bw-based
    auto-bw: disabled(0/115) 0  Bandwidth Requested: 0
.
.
.
Name: te3640-17-c_t222              (Tunnel33) Destination: 192.168.100.22
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 1, type dynamic (Basis for Setup, path weight 10)
  Config Parameters:
    Bandwidth: 200 kbps (Global)   Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: TE                                            !!Note metric type
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 0   bw-based
    auto-bw: disabled(0/115) 0  Bandwidth Requested: 0
.
.
.
```

**Step 4** **exit**

Use this command to return to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

# Configuration Examples for Configuring a Path Calculation Metric for Tunnels

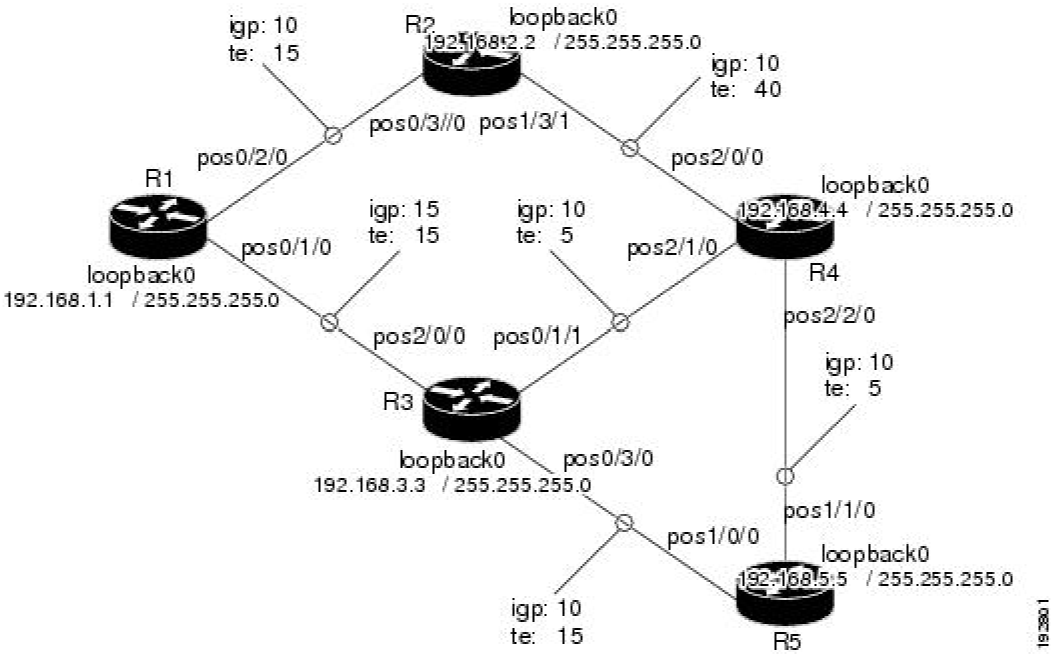


## Example Configuring Link Type and Metrics for Tunnel Path Selection

The section illustrates how to configure the link metric type to be used for tunnel path selection, and how to configure the link metrics themselves. The configuration commands included focus on specifying the metric type for path calculation and assigning metrics to links. Additional commands are required to fully configure the example scenario: for example, the IGP commands for traffic engineering and the link interface commands for enabling traffic engineering and specifying available bandwidth.

The examples in this section support the simple network technology shown in the figure below.

*Figure 4* *Network Topology*




In the figure above:

- Tunnel1 and Tunnel2 run from R1 (headend) to R4 (tailend).
- Tunnel3 runs from R1 to R5.
- Path calculation for Tunnel1 and Tunnel3 should use a metric that represents link delay because these tunnels carry voice traffic.
- Path calculation for Tunnel2 should use IGP metrics because MPLS TE carries data traffic with no delay requirement.

Configuration fragments follow for each of the routers that illustrate the configuration relating to link metrics and their use in tunnel path calculation. TE metrics that represent link delay must be configured for the network links on each of the routers, and the three tunnels must be configured on R1.

These configuration fragments force Tunnel1 to take path R1-R3-R4, Tunnel2 to take path R1-R2-R4, and Tunnel3 to take path R1-R3-R4-R5 (assuming the links have sufficient bandwidth to accommodate the tunnels).

### R1 Configuration

The following example shows how to configure the tunnel headend (R1) for Tunnel1, Tunnel2, and Tunnel3 in the figure above:

```
interface pos0/1/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos0/2/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface Tunnel1                               !Tunnel1 uses TE metric (default)
                                                !for path selection
ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
```

```
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
interface Tunnel2                                 !Tunnel2 uses IGP metric
                                                  !for path selection
ip unnumbered loopback0
tunnel destination 192.168.4.4 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng path-selection-metric igp !Use IGP cost for path selection.
interface Tunnel3                                  !Tunnel3 uses TE metric (default)
                                                   !for path selection
ip unnumbered loopback0
tunnel destination 192.168.5.5 255.255.255.0
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 dynamic
```

### R2 Configuration

The following example shows how to configure R2 in the figure above:

```
interface pos0/3/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos1/3/1
mpls traffic-eng administrative-weight 40       !TE metric different from IGP metric
```

### R3 Configuration

The following example shows how to configure R3 in the figure above:

```
interface pos2/0/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos0/3/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos0/1/1
mpls traffic-eng administrative-weight 5        !TE metric different from IGP metric
```

### R4 Configuration

The following example shows how to configure R4 in the figure above:

```
interface pos2/0/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos2/1/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos2/2/0
mpls traffic-eng administrative-weight 5        !TE metric different from IGP metric
```

### R5 Configuration

The following example shows how to configure R5 in the figure above:

```
interface pos1/0/0
mpls traffic-eng administrative-weight 15       !TE metric different from IGP metric
interface pos1/1/0
mpls traffic-eng administrative-weight 5        !TE metric different from IGP metric
```

# Additional References

### Related Documents

| Related Topic | Document Title |
| --- | --- |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Configuration tasks for IS-IS and OSPF | *Cisco IOS XE IP Routing Protocols Configuration Guide* |
| IS-IS and OSPF commands | *Cisco IOS IP Routing Protocols Command Reference* |
| Configuration tasks for MPLS and MPLS TE | *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* |
| MPLS TE commands | *Cisco IOS Multiprotocol Label Switching Command Reference* |
| Configuration tasks for tunnels | • *Cisco IOS XE Interface and Hardware Component Configuration Guide*<br>• *Cisco IOS XE Multiprotocol Label Switching Configuration Guide* |
| Tunnel configuration commands | • *Cisco IOS Interface and Hardware Component Command Reference*<br>• *Cisco IOS XE Multiprotocol Label Switching Command Reference* |

### Standards

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

### MIBs

| MIB | MIBs Link |
| --- | --- |
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>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. | - |

### Technical Assistance

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

# Feature Information for MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels

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 2 Feature Information for MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels | Cisco IOS XE Release 2.3 | The MPLS Traffic Engineering--Configurable Path Calculation Metric for Tunnels feature enables the user to control the metric used in path calculation for traffic engineering (TE) tunnels on a per-tunnel basis. Certain tunnels are used to carry voice traffic, which requires low delay, and other tunnels are used to carry data. A TE link metric can be used to represent link delay and configure tunnels that carry voice traffic for path calculation and configure tunnels that carry data to use the Interior Gateway Protocol (IGP) metric for path calculation.<br>In Cisco IOS XE Release 12.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |
| | | The following commands were introduced or modified: **mpls traffic-eng path-selection metric**, **tunnel mpls traffic-eng path-selection metric**. |

# MPLS Traffic Engineering--Scalability Enhancements

The MPLS Traffic Engineering--Scalability Enhancement feature improves scalability performance for large numbers of traffic engineering tunnels.

These improvements allow an increase in the number of traffic engineering (TE) tunnels a router can support when the router is configured as a tunnel headend. Additionally, when the router is configured as a tunnel midpoint, the enhancements reduce the time required to establish large numbers of TE tunnels.

This feature module contains information about and instructions on how to configure the Multiprotocol Label Switching (MPLS) traffic engineering scalability enhancements.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering--Scalability Enhancements

Your network must support the following Cisco IOS XE features before you enable MPLS traffic engineering:

- MPLS
- Cisco Express Forwarding
- Intermediate System-to-Intermediate System (IS-IS) or Open Shortest Path First (OSPF)

# Restrictions for MPLS Traffic Engineering--Scalability Enhancements

The number of tunnels that a particular platform can support can vary depending on:

- The types of interfaces that the tunnels traverse
- The manner in which the Resource Reservation Protocol (RSVP) message pacing feature is configured
- MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/ instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

# Information About MPLS Traffic Engineering--Scalability Enhancements



## Scalability Enhancements for Traffic Engineering Tunnels

Scalability performance is improved for large numbers of traffic engineering tunnels, and includes the following enhancements:

- Increase the number of traffic engineering tunnels a router can support when configured as a tunnel headend and when configured as a tunnel midpoint
- Reduce the time required to establish large numbers of traffic engineering tunnels

## RSVP Rate Limiting

A burst of RSVP traffic engineering signaling messages can overflow the input queue of a receiving router, causing some messages to be dropped. Dropped messages cause a substantial delay in completing label switched path (LSP) signaling.

This MPLS Traffic Engineering--Scalability Enhancements feature provides an enhancement mechanism that controls the transmission rate for RSVP messages and reduces the likelihood of input drops on the receiving router. The default transmission rate is 200 RSVP messages per second to a given neighbor. The rate is configurable.

# Improved Recovery Response for Signaling and Management of MPLS Traffic Engineering Tunnels

The MPLS Traffic Engineering--Scalability Enhancements feature improves the recovery response for signaling and management of MPLS TE tunnels. LSP recovery responsiveness is improved when a link used by an LSP fails:

- When the upstream end of a failed link detects the failure, the software generates an RSVP No Route path error message. This enables the LSP headend to detect the link failure and initiate recovery, even when the Interior Gateway Protocol (IGP) update announcing the link failure is delayed.
- The LSP headend marks the link in question so that subsequent constraint-based shortest path first (SPF) calculations ignore the link until either a new IGP update arrives or a configurable timeout occurs. This ensures that resignaling to restore the LSP avoids the failed link.

# IS-IS and MPLS Traffic Engineering Topology Database Interactions

The MPLS Traffic Engineering--Scalability Enhancements feature reduces the interval between when the IS-IS protocol receives an IGP update and when it delivers the update to the MPLS traffic engineering topology database.

Before the MPLS Traffic Engineering--Scalability Enhancements feature was introduced, when IS-IS received a new LSP that contained traffic engineering type, length, value (TLV) objects, a delay of several seconds could occur before IS-IS passed the traffic engineering TLVs to the traffic engineering database. The purpose of the delay was to provide better scalability during periods of network instability and to give the router an opportunity to receive more fragments of the LSP before passing the information to the traffic engineering database. However, this delay increased the convergence time for the traffic engineering database.

With the MPLS Traffic Engineering--Scalability Enhancements feature, IS-IS extracts traffic engineering TLVs from received LSPs and passes them to the traffic engineering database immediately. The exception to this occurs when there are large numbers of LSPs to process and it is important to limit CPU consumption, such as during periods of network instability. The parameters that control IS-IS delivery of traffic engineering TLVs to the traffic engineering topology database are configurable.

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/ instance.

# Improved Counter Capabilities for MPLS TE Tunnels Events and RSVP Signaling

With the MPLS Traffic Engineering--Scalability Enhancements feature, diagnostic and troubleshooting capabilities for MPLS traffic engineering tunnels and RSVP are improved:

- Counters record tunnel headend error events such as no route (link down), preemption, and insufficient bandwidth on a per-tunnel basis.
- Counters record RSVP messages. The counters are per-interface and record the number of RSVP messages of each type sent and received on the interface.

## Benefits of MPLS Traffic Engineering--Scalability Enhancements

The MPLS Traffic Engineering--Scalability Enhancements feature provides the following benefits:

- Increased scalability--Up to 600 MPLS traffic engineering tunnel headends are supported. Up to 10,000 traffic engineering tunnel midpoints are supported, with up to 5000 midpoints per interface.
- Faster recovery after failure conditions--Message pacing provides a mechanism to throttle RSVP control messages so that they are less likely to be dropped. This results in a faster recovery from failure conditions when many MPLS traffic engineering tunnels are being set up.
- Improved reroute time--When a traffic engineering tunnel is down, the headend router needs to be notified so that it can signal for a new LSP for the tunnel along an alternate path. The headend router does not have to wait for an IGP update to signal for a new LSP for the tunnel along an alternate path.
- Improved tunnel setup time--Fewer control messages and tunnel setup messages are dropped. This reduces the average time required to set up tunnels.

# How to Configure MPLS Traffic Engineering--Scalability Enhancements



## Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements

Perform the following task to enable RSVP rate limiting for MPLS traffic engineering scalability enhancements. RSVP rate limiting maintains, on an outgoing interface basis, a count of messages that were dropped because the output queue for the interface used for rate limiting was full.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling rate-limit** [**burst** *number*] [**limit** *number*] [**maxsize** *bytes*] [**period** *ms*]
4. **end**
5. **show ip rsvp neighbor**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip rsvp signalling rate-limit** [**burst** *number*] [**limit** *number*] [**maxsize** *bytes*] [**period** *ms*]<br><br>**Example:**<br>`Router(config)# ip rsvp signalling rate-limit burst 5 maxsize 3 period 2` | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.<br>• The **burst** *number*keyword and argument pair indicates the maximum number of RSVP messages sent to a neighboring router during each interval. The range is from 1 to 5000. The default is 8.<br>• The **limit** *number* keyword and argument pair indicates the maximum number of messages to send per queue interval when the number of messages sent is less than the number of messages to be sent normally. The range is 1 to 5000. The default is 37.<br>• The **maxsize** *bytes* keyword and argument pair indicates the maximum size of the message queue, in bytes. The range is 1 to 5000. The default is 2000.<br>• The **period** *ms* keyword and argument pair indicates the length of the interval (time frame) in milliseconds (ms). The range is 10 to 5000. The default is 20. |
| Step 4 | **end**<br><br>**Example:**<br>`Router(config)# end` | Exits to privileged EXEC mode. |
| Step 5 | **show ip rsvp neighbor**<br><br>**Example:**<br>`Router# show ip rsvp neighbor` | Displays current RSVP neighbors.<br>Use this command to verify that RSVP message pacing is enabled. |

# Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels

Perform this task to manage link failure timeouts for MPLS traffic engineering tunnels.

This allows the configuration of a timeout during which the router ignores a link in its path calculation to avoid paths that contain a failed link and are likely to fail when signaled.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng topology holddown sigerr** *seconds*
4. **end**
5. **show mpls traffic-eng topology** [**brief**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **mpls traffic-eng topology holddown sigerr** *seconds*<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng topology holddown sigerr 15` | Specifies the amount of time that a router ignores a link in its traffic engineering topology database in tunnel path Constrained Shortest Path First (CSPF) computations following a traffic engineering tunnel error on the link.<br><br>• The *seconds* argument specifies the length of time (in seconds) a router should ignore a link during tunnel path calculations following a traffic engineering tunnel error on the link. The range is 0 to 300. The default is 10. |
| **Step 4** | **end**<br><br>**Example:**<br><br>`Router(config)# end` | Exits to privileged EXEC mode. |
| **Step 5** | **show mpls traffic-eng topology** [**brief**]<br><br>**Example:**<br><br>`Router# show mpls traffic-eng topology brief` | Displays the MPLS traffic engineering global topology as currently known at this node.<br><br>• The **brief** keyword provides a less detailed version of the topology. |

# Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database

Perform the following task to control IS-IS and MPLS traffic engineering topology database interactions. This reduces the interval time between when the IS-IS protocol receives an IGP update and when IS-IS delivers the update to the MPLS traffic engineering topology database, which reduces convergence time for the database.

**Note** MPLS traffic engineering supports only a single IGP process/instance. Multiple IGP processes/instances are not supported and MPLS traffic engineering should not be configured in more than one IGP process/instance.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router isis** [*area-tag*]
4. **mpls traffic-eng scanner** [**interval** *seconds*] [**max-flash** *LSPs*]
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **router isis** [*area-tag*]<br><br>**Example:**<br><br>`Router(config)# router isis` | Enables the IS-IS routing protocol and specifies an IS-IS process.<br><br>• The *area-tag* argument is a meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.<br><br>**Note** This argument is Required for multiarea IS-IS configuration and optional for conventional IS-IS configuration. |

| | Command or Action | Purpose |
|---|---|---|
| Step 4 | **mpls traffic-eng scanner** [**interval** *seconds*] [**max-flash** *LSPs*]<br><br>**Example:**<br><br>`Router(config-router)# mpls traffic-eng scanner interval 5 max-flash 100` | Specifies how often IS-IS extracts traffic engineering TLVs from flagged LSPs and passes them to the traffic engineering topology database, and specifies the maximum number of LSPs that the router can process immediately.<br>• The **interval** *seconds* keyword and argument specify the frequency, in seconds, at which IS-IS sends traffic engineering TLVs into the traffic engineering database. The range is 1 to 60. The default is 5.<br>• The **max-flash** *LSPs* keyword and argument specify the maximum number of LSPs that the router can process immediately without incurring a delay. The range is 0 to 200. The default is 15. |
| Step 5 | **end**<br><br>**Example:**<br><br>`Router(config-router)# end` | Exits to privileged EXEC mode. |

# Monitoring and Maintaining MPLS TE Scalability Enhancements

### SUMMARY STEPS

1. **enable**
2. **show ip rsvp neighbor** [**detail**]
3. **show ip rsvp counters** [**summary**]
4. **clear ip rsvp counters**
5. **clear ip rsvp signalling rate-limit**
6. **show mpls traffic-eng tunnels statistics**
7. **clear mpls traffic-eng tunnels counters**
8. **show mpls traffic-eng topology** [**brief**]
9. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show ip rsvp neighbor** [**detail**]

Use this command to verify that RSVP message pacing is turned on. For example:

**Example:**

```
Router# show ip rsvp neighbor detail
Neighbor:10.0.0.1
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
Refresh Reduction:
      Remote epoch:0x1BFEA5
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:1059
      Last rcvd message:00:00:04
Neighbor:10.0.0.2
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
    Refresh Reduction:
      Remote epoch:0xB26B1
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:945
      Last rcvd message:00:00:05
```

**Step 3** **show ip rsvp counters** [**summary**]

Use this command to display the counts of RSVP messages that were sent and received. For example:

**Example:**

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit                          Recv      Xmit
    Path                 110        15    Resv                    50        28
    PathError              0         0    ResvError                0         0
    PathTear               0         0    ResvTear                 0         0
    ResvConf               0         0    RTearConf                0         0
    Ack                    0         0    Srefresh                 0         0
    Hello               5555      5554    IntegrityChalle          0         0
    IntegrityRespon        0         0    DSBM_WILLING             0         0
    I_AM_DSBM              0         0
    Unknown                0         0    Errors                   0         0
Recv Msg Queues               Current       Max
    RSVP                            0         2
    Hello (per-I/F)                 0         1
    Awaiting Authentication         0         0
```

**Step 4** **clear ip rsvp counters**

Use this command to clear (set to zero) all IP RSVP counters that are being maintained. For example:

**Example:**

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

**Step 5** **clear ip rsvp signalling rate-limit**

Use this command to clear (set to zero) counts of the messages that message pacing was forced to drop because the output queue for the interface used for message pacing was full. For example:

**Example:**

```
Router# clear ip rsvp signalling rate-limit
```

**Step 6** **show mpls traffic-eng tunnels statistics**

Use this command to display event counters for one or more MPLS traffic engineering tunnels. For example:

**Example:**

```
Router# show mpls traffic-eng tunnels statistics
Tunnel1001 (Destination 10.8.8.8; Name Router_t1001)
  Management statistics:
    Path:    25 no path, 1 path no longer valid, 0 missing ip exp path
    5 path changes
    State:    3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens:    2 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:    0 no b/w, 0 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other

...
```

**Example:**

```
Tunnel7050 (Destination 10.8.8.8; Name Router_t7050)
  Management statistics:
    Path:     19 no path, 1 path no longer valid, 0 missing ip exp path
    3 path changes
    State:     3 transitions, 0 admin down, 1 oper down
  Signalling statistics:
    Opens:     2 succeeded, 0 timed out, 0 bad path spec
    0 other aborts
    Errors:    0 no b/w, 0 no route, 0 admin
    0 bad exp route, 0 rec route loop, 0 other
```

**Step 7** **clear mpls traffic-eng tunnels counters**

Use this command to clear counters for all MPLS traffic engineering tunnels. For example:

**Example:**

```
Router# clear mpls traffic-eng tunnels counters
Clear traffic engineering tunnel counters [confirm]
```

**Step 8** **show mpls traffic-eng topology** [**brief**]

Use this command to display the MPLS traffic engineering topology database. For example:

**Example:**

```
Router# show mpls traffic-eng topology brief
My_System_id:0000.0000.0003.00 (isis  level-2)
Signalling error holddown:10 sec Global Link Generation 9
IGP Id:0000.0000.0003.00, MPLS TE Id:10.0.3.1 Router Node  (isis
level-2)
      link[0]:Point-to-Point, Nbr IGP Id:0000.0000.0004.00,
nbr_node_id:2, gen:9
          frag_id 0, Intf Address:10.0.0.33, Nbr Intf Address:10.0.0.34
          TE metric:10, IGP metric:10, attribute_flags:0x0
          SRLGs:1 2
```

**Step 9** **exit**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

# Configuration Examples for MPLS Traffic Engineering--Scalability Enhancements



## Example Enabling RSVP Rate Limiting for MPLS Traffic Engineering Scalability Enhancements

The following examples show how to enable RSVP rate limiting for MPLS traffic engineering scalability enhancements:

```
configure terminal
 ip rsvp signalling rate-limit
 end
```

The following is sample output that traffic engineering displays when RSVP rate limiting is enabled:

```
Router# show ip rsvp signalling rate-limit
Rate Limiting: enabled
  Burst: 10
  Limit: 37
  Maxsize: 5000
  Period (msec): 100
  Max rate (msgs/sec): 100
```

The following example shows how to configure a router to send a maximum of 5 RSVP traffic engineering signaling messages in 1 second to a neighbor. The size of the output queue is 35.

```
configure terminal
 ip rsvp signalling rate-limit
period 1 burst 5 maxsize 35
```

## Example Managing Link Failure Timeouts for MPLS Traffic Engineering Tunnels

The following example shows how to manage link failure timeouts for MPLS traffic engineering tunnels:

```
configure terminal
 mpls traffic-eng topology holddown sigerr 15
 end
```

In this example, the link hold-down time for signaling errors is set to 15 seconds.

## Example Controlling IS-IS Communication with the MPLS Traffic Engineering Topology Database

The following example shows how to control IS-IS communication with the MPLS traffic engineering topology database:

```
configure terminal
router isis
 mpls traffic-eng scanner interval 5 max-flash 50
 end
```

In this example, the router is enabled to process up to 50 IS-IS LSPs without any delay.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Quality of service | • *Cisco IOS Quality of Service Solutions Command Reference*<br>• *Cisco IOS XE Quality of Service Solutions Configuration Guide*, Release 2 |
| MPLS | • *Cisco IOS Multiprotocol Label Switching Command Reference*<br>• *Cisco IOS XE Multiprotocol Label Switching Configuration Guide*, Release 2 |

### Standards

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

### MIBs

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

### RFCs

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

### Technical Assistance

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

# Feature Information for MPLS Traffic Engineering--Scalability Enhancements

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 3 Feature Information for MPLS Traffic Engineering--Scalability Enhancements*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering--Scalability Enhancements | Cisco IOS XE Release 2.3 | The MPLS Traffic Engineering--Scalability Enhancements feature improves scalability performance for large numbers of traffic engineering tunnels.<br>These improvements allow an increase in the number of traffic engineering (TE) tunnels a router can support when the router is configured as a tunnel headend. Additionally, when the router is configured as a tunnel midpoint, the enhancements reduce the time required to establish large numbers of TE tunnels.<br>This feature module contains information about and instructions on how to configure the Multiprotocol Label Switching (MPLS) traffic engineering scalability enhancements.<br>In Cisco IOS XE Release 2.1, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |
| | | The following commands were introduced or modified: **clear ip rsvp counters**, **clear ip rsvp signalling rate-limit**, **clear mpls traffic-eng tunnel counters**, **ip rsvp signalling rate-limit**, **mpls traffic-eng scanner**, **mpls traffic-eng topology holddown sigerr**, **show ip rsvp counters**, and **show mpls traffic-eng tunnels statistics**. |

# Glossary

**Cisco Express Forwarding** --A means for accelerating the forwarding of packets within a router, by storing route lookup information in several data structures instead of in a route cache.

**CLNS** --Connectionless Network Services. The Open System Interconnection (OSI) network layer service that does not require a circuit to be established before the data is transmitted. CLNS routes messages to their destination independently of any other messages.

**CSPF** --Constrained Shortest Path First. A routing protocol that calculates the shortest path based on a set of constraints, such as a minimum bandwidth requirement, maximum number of nodes, or nodes to include or exclude.

**enterprise network** --A large and diverse network connecting most major points in a company or other organization.

**headend** --The endpoint of a broadband network. All stations send toward the headend; the headend then sends toward the destination stations.

**IGP** --Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Interior Gateway Routing protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**interface** --A network connection.

**IS-IS** --Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol based on DECnet Phase V routing, where ISs (routers) exchange routing information based on a single metric, to determine the network topology.

**LSP** --label switched path.A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through label switching mechanisms. A label switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**message-pacing** --The former name of the rate limiting feature.

**MPLS** --Multiprotocol Label Switching (formerly known as tag switching). A method for directing packets primarily through Layer 2 switching rather than Layer 3 routing. In MPLS, packets are assigned short fixed-length labels at the ingress to an MPLS cloud by using the concept of forwarding equivalence classes. Within the MPLS domain, the labels are used to make forwarding decisions mostly without recourse to the original packet headers.

**OSPF** --Open Shortest Path First. A link-state, hierarchical Interior Gateway Protocol (IGP) routing protocol. derived from the Intermediate System-Intermediate System (IS-IS) protocol. OSPF features are least-cost routing, multipath routing, and load balancing.

**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.

**RSVP** --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network.

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

**TLV** --type, length, value objects. TLVs are used in data communication to provide optional information. The type field indicates the type of items in the value field. The length field indicates the length of the value field. The value field is the data portion of the packet.

**topology** --The physical arrangement of network nodes and media within an enterprise networking structure.

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

**traffic engineering tunnel** --A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing would cause the tunnel to take.

# MPLS Traffic Engineering--LSP Attributes

This document describes how to configure label switched path (LSP) attributes for path options associated with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.

The MPLS Traffic Engineering--LSP Attributes feature is an extension to MPLS TE that provides an LSP Attribute list feature and a Path Option for Bandwidth Override feature. These features provide flexibility in the configuration of LSP attributes for MPLS TE tunnel path options. Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a Path Option for Bandwidth Override.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering--LSP Attributes

TheMPLS Traffic Engineering--LSP Attributes feature requires that you configure an MPLS TE tunnel before you configure either an LSP Attribute List or a Path Option for Bandwidth Override feature.

## Restrictions for MPLS Traffic Engineering--LSP Attributes

Reoptimization between path options with different bandwidth pool types (subpool versus global pool) and different priorities is not supported. Specifically,

- With the Path Option for Bandwidth Override feature, you need to configure bandwidth for path options with the same bandwidth pool as configured for the tunnel.
- With the LSP Attribute List feature, you need to configure both a bandwidth pool and priority for path options that are consistent with the bandwidth pool and priority configured on the tunnel or in other path options used by the tunnel.

# Information About MPLS Traffic Engineering--RSVP Hello State Timer



## MPLS Traffic Engineering--LSP Attributes Benefits

The MPLS Traffic Engineering--LSP Attributes feature provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features have the following benefits:

- The LSP Attributes List feature provides the ability to configure values for several LSP-specific path options for TE tunnels.
- One or more TE tunnels can specify specific path options by referencing an LSP Attribute List.
- LSP attribute lists make the MPLS TE user interface more flexible, easier to use, and easier to extend and maintain.
- The Path Option for Bandwidth Override feature provides a single command that allows a TE tunnel to fall back temporarily to path options that can reduce bandwidth constraints.

# Traffic Engineering Bandwidth and Bandwidth Pools

MPLS traffic engineering allows constraint-based routing (CBR) of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Regular TE tunnel bandwidth is called the global pool. Subpool bandwidth is a portion of the global pool. Subpool bandwidth is not reserved from the global pool if it is not in use. Therefore, subpool tunnels require a higher priority than nonsubpool tunnels.

You can configure the LSP Attribute bandwidth path option to use either global pool (default) or subpool bandwidth. The bandwidth value for the path option may be any valid value and the pool does not have to be the same as that configured on the tunnel.

**Note** When you configure bandwidth for path options with the **bandwidth** [**sub-pool** | **global**] *kbps* command, use either all subpool bandwidths or all global-pool bandwidths.

You can configure bandwidth on both dynamic and explicit path options using either the LSP Attribute List feature or the Path Option for Bandwidth Override feature. The commands that enable these features are exclusive of each other. If bandwidth is the only LSP attribute that you need to set on the path option, then use the command to enable the feature. This is the simplest way to configure multiple path options with decreasing bandwidth constraints. Once the **bandwidth** keyword is entered on the **tunnelmplstraffic-engpath-option** command in interface configuration mode, you cannot configure an LSP Attribute List for that path option.

# Tunnel Attributes and LSP Attributes

Cisco IOS XE tunneling interfaces have many parameters associated with MPLS TE. Typically, you configure these parameters with **tunnel mpls traffic-eng** commands in interface configuration mode. Many of these commands determine tunnel-specific properties, such as the load-sharing factor for the tunnel. These commands configure parameters that are unrelated to the particular LSP in use by the tunnel. However, some of the tunneling parameters apply to the LSP that the tunnel uses. You can configure the LSP-specific properties using an LSP Attribute list.

# LSP Attributes and the LSP Attribute List

An LSP Attribute list can contain values for each LSP-specific parameter that is configurable for a TE tunnel. You configure an LSP attribute list with the **mplstraffic-englspattributes***string* command, where *string* identifies the attribute list. The LSP attributes that you can specify include the following:

- Attribute flags for links that make up the LSP (**affinity** command)
- Automatic bandwidth configuration (**auto-bw** command)
- LSP bandwidth--global pool or subpool (**bandwidth** command)
- Disable reoptimization of the LSP (**lockdown** command)
- LSP priority (**priority** command)
- Protection failure (**protection** command)
- Record the route used by the LSP (**record-route** command)

# LSP Attribute Lists Management

The MPLS Traffic Engineering--LSP Attributes feature also provides commands that help you manage LSP Attribute lists. You can do the following:

- Relist all attribute list entries (**list** command)
- Remove a specific attribute from the list (**no***attribute* command)

The **exit** command exits from the LSP attributes configuration submode and returns you to global configuration mode.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

# Autobandwidth and Path Option for Bandwidth Override

If Traffic Engineering automatic bandwidth (autobandwidth) adjustment is configured for a tunnel, traffic engineering automatically adjusts the bandwidth allocation for the traffic engineering tunnel based on its measured usage of the bandwidth of the tunnel.

Traffic engineering autobandwidth samples the average output rate for each tunnel marked for automatic bandwidth adjustment. For each marked tunnel, it periodically adjusts the allocated bandwidth for the tunnel to be the largest sample for the tunnel since the last adjustment. The default reoptimization setting in the MPLS AutoBandwidth feature is every 24 hours

The frequency with which tunnel bandwidth is adjusted and the allowable range of adjustments is configurable on a per-tunnel basis. In addition, the sampling interval and the interval over which to average tunnel traffic to obtain the average output rate is user-configurable on a per-tunnel basis.

The Path Option for Bandwidth Override feature allows you to override the bandwidth configured on a TE tunnel. This feature also overrides bandwidth configured or recalculated by automatic bandwidth adjustment if the path option in effect has bandwidth override enabled.

# Constraint-Based Routing and Path Option Selection

MPLS traffic engineering automatically establishes and maintains LSPs across the backbone by using the Resource Reservation Protocol (RSVP). The path that an LSP uses is determined by the LSP resource requirements and network resources, such as bandwidth. Traffic engineering tunnels are calculated at the LSP head based on a fit between required and available resources (constraint-based routing).

Without the Path Option for Bandwidth Override feature, a TE tunnel establishes an LSP based on dynamic or explicit path options in order of preference. However, the bandwidth and other attributes configured on the TE tunnel allow the setup of an LSP only if LSP path options satisfy the constraints. If a path cannot be found that satisfies the configured path options, then the tunnel is not set up.

The Path Option for Bandwidth Override feature provides a fallback path option that allows overriding the bandwidth configured on the TE tunnel interface. For example, you can configure a path option that sets the bandwidth to zero (0) effectively removing the bandwidth constraint imposed by the constraint-based routing calculation.

# Tunnel Reoptimization and Path Option Selection

Reoptimization occurs when a device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP. If the signaling is successful, the device replaces the older LSP with the new, better LSP.

Reoptimization can be triggered by a timer, the issuance of an **mplstraffic-engreoptimize** command, or a configuration change that requires the resignalling of a tunnel. The MPLS AutoBandwidth feature, for example, uses a timer to set the frequency of reoptimization based on the bandwidth path option attribute. The Path Option for Bandwidth Override feature allows for the switching between bandwidth configured on the TE tunnel interface and bandwidth configured on a specific path option. This increases the success of signaling an LSP for the TE tunnel.

With bandwidth override configured on a path option, the traffic engineering software attempts to reoptimize the bandwidth every 30 seconds to reestablish the bandwidth configured on the tunnel (see the Configuring a Path Option for Bandwidth Override, page 92).

You can disable reoptimization of an LSP with the **lockdown** command in an LSP Attribute list. You can apply the LSP Attribute list containing the **lockdown** command to a path option with the **tunnelmplstraffic-engpath-option** command.

**Note** When you configure bandwidth for path options with the **bandwidth** [**sub-pool** | **global**] *kpbs* command, use either all subpool bandwidths or all global-pool bandwidths. Do not mix subpool and nonsubpool bandwidths, otherwise the path option does not reoptimize later.

# Path Option Selection with Bandwidth Override

The Path Option for Bandwidth Override feature allows you to configure bandwidth parameters on a specific path option with the **bandwidth** keyword on the **tunnelmplstraffic-engpath-option** command. When an LSP is signaled using a path option with a configured bandwidth, the bandwidth associated with the path option is signaled instead of the bandwidth configured directly on the tunnel.

This feature provides you with the ability to configure multiple path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

The following configuration shows three **tunnelmplstraffic-engpath-option** commands:

```
tunnel mpls traffic-eng bandwidth 1000
tunnel mpls traffic-eng path-option 1 explicit name path1
tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
```

The device selects a path option for an LSP in order of preference, as follows:

- The device attempts to signal an LSP using path options starting with path option 1.

The device attempts to signal an LSP with the 1000 kbps bandwidth configured on the tunnel interface because path-option 1 has no bandwidth configured.

- If 1000 kbps bandwidth is not available over the network, the device attempts to establish an LSP using path-option 2.

Path option 2 has a bandwidth of 500 kbps configured. This reduces the bandwidth constraint from the original 1000 kbps configured on the tunnel interface.

- If 500 kbps is not available, the device attempts to establish an LSP using path-option 3.

Path-option 3 is configured as dynamic and has bandwidth 0. The device establishes the LSP if an IP path exists to the destination and all other tunnel constraints are met.

# Default Path Option Attributes for TE Tunnels Using LSP Attribute Lists

Values for path option attributes for a TE tunnel are determined in this manner:

- LSP attribute list values referenced by the path option take precedence over the values configured on the tunnel interface.
- If an attribute is not specified in the LSP attribute list, the device uses the attribute in the tunnel configuration. LSP attribute lists do not have defaults.
- If the attribute is not configured on the tunnel, then the device uses the tunnel default value, as follows:

{affinity= affinity 0 mask 0,

auto-bw= no auto-bw,

bandwidth= bandwidth 0,

lockdown= no lockdown,

priority= priority 7 7,

protection fast-reroute= no protection fast-reroute,

record-route= no record-route

.

.

.

}

# How to Configure MPLS Traffic Engineering--LSP Attributes



## Configuring an LSP Attribute List

Perform this task to configure a label switched path (LSP) attribute list with the desired attributes to be applied on a path option. Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. The LSP attribute list provides a user interface that is flexible, easy to use, and easy to extend and maintain for the configuration of MPLS TE tunnel path options.

LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask** *value*]
5. **auto-bw** [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]
6. **bandwidth** [**sub-pool**| **global**] *kbps*
7. **list**
8. **lockdown**
9. **priority** *setup-priority* [*hold-priority*]
10. **protection fast-reroute**
11. **record-route**
12. **no** *sub-command*
13. **exit**
14. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **mpls traffic-eng lsp attributes** *string*<br><br>**Example:**<br>`Router(config)# mpls traffic-eng lsp attributes 1` | Configures an LSP attribute list and enters LSP Attributes configuration mode.<br>• The *string* argument identifies a specific LSP attribute list. |

| | Command or Action | Purpose |
|---|---|---|
| Step 4 | **affinity** *value* [**mask** *value*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# affinity 0 mask 0` | (Optional) Specifies attribute flags for links comprising an LSP.<br>• The *value* argument is a value required for links that make up an LSP. Values of the bits are either 0 or 1.<br>• The **mask** *value* keyword argument combination indicates which attribute values should be checked.<br>  ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.<br>  ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match. |
| Step 5 | **auto-bw** [**frequency** *secs*] [**max-bw** *kbps*] [**min-bw** *kbps*] [**collect-bw**]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# auto-bw` | (Optional) Specifies automatic bandwidth configuration.<br>• The **frequency** *secs* keyword argument combination specifies the interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds.<br>• The **max-bw** *kbps* keyword argument combination specifies the maximum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295.<br>• The **min-bw** *kpbs* keyword argument combination specifies the minimum automatic bandwidth, in kbps, for this path option. The value can be from 0 to 4294967295.<br>• The **collect-bw** keyword collects output rate information for the path option, but does not adjust the bandwidth of the path option. |
| Step 6 | **bandwidth** [**sub-pool**\| **global**] *kbps*<br><br>**Example:**<br><br>`Router(config-lsp-attr)# bandwidth 5000` | (Optional) Specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. |
| Step 7 | **list**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# list` | (Optional) Displays the contents of the LSP attribute list. |
| Step 8 | **lockdown**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# lockdown` | (Optional) Disables reoptimization of the LSP. |

| | Command or Action | Purpose |
|---|---|---|
| Step 9 | **priority** *setup-priority* [*hold-priority*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# priority 1 1` | (Optional) Specifies the LSP priority.<br><br>• The *setup-priority* argument is used when signaling an LSP to determine which existing LSPs can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.<br>• The *hold-priority* argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority. |
| Step 10 | **protection fast-reroute**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# protection fast-reroute` | (Optional) Enables failure protection on the LSP. |
| Step 11 | **record-route**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# record-route` | (Optional) Records the route used by the LSP. |
| Step 12 | **no** *sub-command*<br><br>**Example:**<br><br>`Router(config-lsp-attr)# no record-route` | (Optional) Removes a specific attribute from the LSP attributes list.<br><br>• The *sub-command*argument names the LSP attribute to remove from the attributes list. |
| Step 13 | **exit**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# exit` | (Optional) Exits from LSP Attributes configuration mode. |
| Step 14 | **end**<br><br>**Example:**<br><br>`Router(config)# end` | (Optional) Exits to privileged EXEC mode. |

## Adding Attributes to an LSP Attribute List

Perform this task to add attributes to an LSP attribute list. The LSP attribute list provides a user interface that is flexible, easy to use, and that can be extended or changed at any time to meet the requirements of your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attributes list and to add or change the required path option attribute.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask***value*]
5. **bandwidth** [**sub-pool** | **global**] *kbps*
6. **priority** *setup-priority* [*hold-priority*]
7. **list**
8. **exit**
9. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **mpls traffic-eng lsp attributes** *string*<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng lsp attributes 1` | Configures an LSP Attribute list and enters LSP Attributes configuration mode.<br><br>• The *string* argument identifies a specific LSP Attribute list. |

| | Command or Action | Purpose |
|---|---|---|
| Step 4 | **affinity** *value* [**mask***value*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# affinity 0 mask 0` | (Optional) Specifies attribute flags for links comprising an LSP.<br>• The *value* argument is a value required for links that make up an LSP. Values of the bits are either 0 or 1.<br>• The **mask***value* keyword argument combination indicates which attribute values should be checked.<br>  ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.<br>  ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the LSP for that bit must match. |
| Step 5 | **bandwidth** [**sub-pool** \| **global**] *kbps*<br><br>**Example:**<br><br>`Router(config-lsp-attr)# bandwidth 1000` | Specifies an LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295. |
| Step 6 | **priority** *setup-priority* [*hold-priority*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# priority 2 2` | Specifies the LSP priority.<br>• The *setup-priority* argument is used when signaling an LSP to determine which existing LSPs can be preempted. Valid values are from 0 to 7, where a lower number indicates a higher priority. Therefore, an LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.<br>• The *hold-priority* argument is associated with an LSP to determine if it should be preempted by other LSPs that are being signaled. Valid values are from 0 to 7, where a lower number indicates a higher priority. |
| Step 7 | **list**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# list` | (Optional) Displays the contents of the LSP attribute list.<br>• Use the **list** command to display the path option attributes added to the attribute list. |
| Step 8 | **exit**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# exit` | (Optional) Exits LSP Attributes configuration mode. |
| Step 9 | **end**<br><br>**Example:**<br><br>`Router(config)# end` | (Optional) Exits to privileged EXEC mode. |

# Removing an Attribute from an LSP Attribute List

Perform this task to remove an attribute from an LSP attribute list. The LSP attributes list provides a means to easily remove a path option attribute that is no longer required for your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attribute list and for the **no***sub-command*command, which is used to remove the specific attribute from the list. Replace the*sub-command* argument with the command that you want to remove from the list.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **no** *sub-command*
5. **list**
6. **exit**
7. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **mpls traffic-eng lsp attributes** *string*<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng lsp attributes 1` | Configures an LSP Attribute list and enters LSP Attributes configuration mode.<br><br>• The *string* argument identifies a specific LSP attribute list. |
| Step 4 | **no** *sub-command*<br><br>**Example:**<br><br>`Router(config-lsp-attr)# no priority` | Removes a specific attribute from the LSP Attribute list.<br><br>• The *sub-command*argument names the LSP attribute to remove from the attributes list. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **list**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# list` | (Optional) Displays the contents of the LSP attribute list.<br><br>• Use the **list** command to verify that the path option attribute is removed from the attribute list. |
| **Step 6** | **exit**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# exit` | (Optional) Exits LSP Attributes configuration mode. |
| **Step 7** | **end**<br><br>**Example:**<br><br>`Router(config)# end` | (Optional) Exits to privileged EXEC mode. |

# Modifying an Attribute in an LSP Attribute List

Perform this task to modify an attribute in an LSP attribute list. The LSP attribute list provides a flexible user interface that can be extended or modified an any time to meet the requirements of your MPLS TE tunnel traffic. LSP Attributes configuration mode is used to display the specific LSP attributes list and to modify the required path option attribute.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string*
4. **affinity** *value* [**mask***value*]
5. **list**
6. **affinity** *value* [**mask***value*]
7. **list**
8. **exit**
9. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **mpls traffic-eng lsp attributes** *string*<br><br>**Example:**<br><br>`Router(config)# mpls traffic-eng lsp attributes 1` | Configures an LSP Attribute list and enters LSP Attributes configuration mode.<br><br>• The *string* argument identifies a specific LSP attribute list. |
| Step 4 | **affinity** *value* [**mask***value*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# affinity 1 mask 1` | Specifies attribute flags for links comprising an LSP.<br><br>• The *value* argument is a value required for links comprising an LSP. Values of bits are either 0 or 1.<br>• The **mask***value* keyword argument combination indicates which attribute values should be checked.<br>  ◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.<br>  ◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match. |
| Step 5 | **list**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# list` | (Optional) Displays the contents of the LSP Attribute list.<br><br>• Use the **list** command to display the path option attributes configured in the attribute list. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **affinity** *value* [**mask***value*]<br><br>**Example:**<br><br>`Router(config-lsp-attr)# affinity 0 mask 0` | Specifies attribute flags for links comprising an LSP.<br>• The *value* argument is a value required for links comprising an LSP. Values of bits are either 0 or 1.<br>• The **mask***value* keyword argument combination indicates which attribute values should be checked.<br>◦ If a bit in the mask is 0, an attribute value of the link or that bit is irrelevant.<br>◦ If a bit in the mask is 1, the attribute value of that link and the required affinity of the tunnel for that bit must match. |
| **Step 7** | **list**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# list` | (Optional) Displays the contents of the LSP attribute list.<br>• Use the **list** command to verify that the path option attributes is modified in the attribute list. |
| **Step 8** | **exit**<br><br>**Example:**<br><br>`Router(config-lsp-attr)# exit` | (Optional) Exits LSP Attributes configuration mode. |
| **Step 9** | **end**<br><br>**Example:**<br><br>`Router(config)# end` | (Optional) Exits to privileged EXEC mode. |

# Deleting an LSP Attribute List

Perform this task to delete an LSP attribute list. You would perform this task when you no longer require the LSP attribute path options specified in the LSP attribute list for an MPLS TE tunnel.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **no mpls traffic-eng lsp attributes** *string*
4. **end**
5. **show mpls traffic-eng lsp attributes** [*string*]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **no mpls traffic-eng lsp attributes** *string*<br><br>**Example:**<br><br>`Router(config)# no mpls traffic-eng lsp attributes 1` | Removes a specified LSP Attribute list from the device configuration.<br><br>• The *string* argument identifies the specific LSP attribute list to remove. |
| Step 4 | **end**<br><br>**Example:**<br><br>`Router(config)# end` | (Optional) Exits to privileged EXEC mode. |
| Step 5 | **show mpls traffic-eng lsp attributes** [*string*]<br><br>**Example:**<br><br>`Router# show mpls traffic-eng lsp attributes` | (Optional) Displays information about configured LSP attribute lists.<br><br>• Use the**showmplstraffic-englspattributes** command to verify that the LSP attribute list was deleted from the router. |

# Verifying Attributes Within an LSP Attribute List

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng lsp attributes** *string* **list**
4. **exit**
5. **end**

## DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **configure terminal**

Use this command to enter global configuration mode. For example:

**Example:**

```
Router# configure terminal
Router(config)#
```

**Step 3** **mpls traffic-eng lsp attributes** *string* **list**

Use this command to enter LSP Attributes configuration mode for a specific LSP attribute list and to verify that the contents of the attributes list are as expected. For example:

**Example:**

```
Router(config)# mpls traffic-eng lsp attributes 1 list
LIST 1
 bandwidth 1000
 priority 1 1
```

**Step 4** **exit**

Use this command to exit LSP Attributes configuration mode. For example:

```
Router(config-lsp-attr)# exit
```

**Example:**

```
Router(config)#
```

**Step 5** **end**

Use this command to exit to privileged EXEC mode. For example:

**Example:**

```
Router(config)# exit
Router#
```

# Verifying All LSP Attribute Lists

Perform this task to verify all configured LSP attribute lists. Use this task to display all LSP attribute lists to verify that the attributes lists that you configured are in operation.

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng lsp attributes** [*string*][**details**]
3. **show running-config** | **begin***text-string*
4. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng lsp attributes** [*string*][**details**]

Use this command to verify that all configured LSP attribute lists are as expected. For example:

**Example:**

```
Router# show mpls traffic-eng lsp attributes
LIST 1
  affinity 1 mask 1
  bandwidth 1000
  priority 1 1
LIST 2
  bandwidth 5000
LIST hipriority
  priority 0 0
!
```

**Step 3** **show running-config** | **begin***text-string*

Use this command to verify that all configured LSP attribute lists are as expected. Use the **begin** command modifier with the**mplstraffic-englsp***text-string*to locate the LSP attributes information in the configuration file. For example:

**Example:**

```
Router# show running-config | begin mpls traffic-eng lsp
mpls traffic-eng lsp attributes 1
  affinity 1 mask 1
  bandwidth 1000
  priority 1 1
!
mpls traffic-eng lsp attributes 2
  bandwidth 5000
!
mpls traffic-eng lsp attributes hipriority
  priority 0 0
```

```
.
.
.
Router#
```

**Step 4** **exit**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

# Associating an LSP Attribute List with a Path Option for an MPLS TE Tunnel

Perform this task to associate an LSP attribute list with a path option for an MPLS TE tunnel. This task is required if you want to apply the LSP attribute list that you configured to path options for your MPLS TE tunnels.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options. LSP attribute lists also provide an easy way to configure multiple TE tunnels to use the same LSP attributes. That is, you can reference the same LSP attribute list to configure LSP-specific parameters for one or more TE tunnels.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mode mpls traffic-eng**
6. **tunnel mpls traffic-eng autoroute announce**
7. **tunnel mpls traffic-eng bandwidth** [**sub-pool**| **global**] *bandwidth*
8. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
9. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
10. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br><br>**Example:**<br><br>`Router(config)# interface tunnel 1` | Configures an interface type and enters interface configuration mode.<br><br>• The *type* argument is the type of interface that you want to configure.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br><br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |
| Step 5 | **tunnel mode mpls traffic-eng**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mode mpls traffic-eng` | Sets the encapsulation mode for the tunnel for MPLS TE. |
| Step 6 | **tunnel mpls traffic-eng autoroute announce**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng autoroute announce` | Specifies that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation. |
| Step 7 | **tunnel mpls traffic-eng bandwidth** [**sub-pool**\| **global**] *bandwidth*<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 1000` | Configures the bandwidth required for an MPLS TE tunnel and assigns it either to the subpool or the global pool.<br><br>• The **sub-pool** keyword indicates a subpool tunnel.<br>• The **global** keyword indicates a global pool tunnel. Entering this keyword is not necessary, for all tunnels are in the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng priority 1 1` | Sets the priority to be used when the system determines which existing tunnels are eligible to be preempted.<br><br>• The *setup-priority* argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted.<br><br>Valid values are from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.<br><br>• The *hold-priority* argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled.<br><br>Valid values are from 0 to 7, where a lower number indicates a higher priority. |
| **Step 9** | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name** *path-name* \| *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1`<br><br>**Example:** | Adds an LSP attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel.<br><br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name** *path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br><br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br><br>• The **attributes** *string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| **Step 10** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |

# Modifying a Path Option to Use a Different LSP Attribute List

Perform this task to modify the path option to use a different LSP Attribute list.

Based on your requirements, you can configure LSP attributes lists with different sets of attributes for different path options or change the set of attributes associated with a path option. The **tunnel mpls traffic-eng path-option** *number* **dynamic attributes** *string* command is used in interface configuration mode to modify the path option to use a different LSP attribute list. The **attributes** and *string* keyword and argument names the new LSP attribute list for the path option specified.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name***path-name* | *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface tunnel 1` | Configures the interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface that you want to configure.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name***path-name* \| *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1` | Adds an LSP Attribute list to specify LSP-related parameters for a path options for an MPLS TE tunnel.<br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name***path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br>• The **attributes***string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |

# Removing a Path Option for an LSP for an MPLS TE Tunnel

Perform this task to remove a path option for an LSP for an MPLS TE tunnel. Use this task to remove a path option for an LSP when your MPLS TE tunnel traffic requirements change.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **no tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name***path-name* | *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br><br>**Example:**<br><br>`Router(config)# interface tunnel 1` | Configures the interface type and enters interface configuration mode.<br><br>• The *type* argument is the type of interface that you want to configure.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br><br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **no tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name***path-name* \| *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# no tunnel mpls traffic-eng path-option 1 dynamic attributes 1` | Removes an LSP Attribute list that specifies LSP-related parameters for a path option for an MPLS TE tunnel.<br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name***path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br><br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br><br>• The **attributes***string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| Step 6 | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |

# Verifying that LSP Is Signaled Using the Correct Attributes

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]
3. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

Use this command to verify that the LSP is signaled using the correct attributes for the specified tunnel. For example:

**Example:**

```
Router# show mpls traffic-eng tunnels tunnel1
Name: Router-t1                      (Tunnel1) Destination: 10.10.10.12
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 2, type explicit path2 (Basis for Setup, path weight 65834)
  Config Parameters:
    Bandwidth: 1000      kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: IGP (global)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 1        bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 2 is active
    BandwidthOverride: enabled   LockDown: disabled  Verbatim: disabled
    Bandwidth Override:
      Signalling: 1        kbps (Global)
      Overriding: 1000        kbps (Global) configured on tunnel
```

The output shows that the following attributes are signaled for tunnel tunnel1: affinity 0 mask 0, auto-bw disabled, bandwidth 1000, lockdown disabled, and priority 1 1.

**Step 3** **exit**

Use this command to return to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

# Configuring a Path Option for Bandwidth Override

This section contains the following tasks for configuring a path option for bandwidth override:

**Note** Once you configure bandwidth as a path-option parameter, you can no longer configure an LSP Attribute list as a path-option parameter.


- Configuring Fallback Bandwidth Path Options for TE Tunnels, page 93
- Modifying the Bandwidth on a Path Option for Bandwidth Override, page 94
- Removing a Path Option for Bandwidth Override, page 96
- Verifying that LSP Is Signaled Using the Correct Bandwidth, page 98

## Configuring Fallback Bandwidth Path Options for TE Tunnels

Perform this task to configure fallback bandwidth path options for a TE tunnel. Use this task to configure path options that reduce the bandwidth constraint each time the headend of a tunnel fails to establish an LSP.

Configuration of the Path Option for Bandwidth Override feature can reduce bandwidth constraints on path options temporarily and improve the chances that an LSP is set up for the TE tunnel. When a TE tunnel uses a path option with bandwidth override, the traffic engineering software attempts every 30 seconds to reoptimize the tunnel to use the preferred path option with the original configured bandwidth. The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the **mplstraffic-engreoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name***path-name* | *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br><br>**Example:**<br>`Router(config)# interface tunnel 1` | Configures an interface type and enters interface configuration mode.<br>• The *type* argument is the type of interface that you want to configure.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |

| | Command or Action | Purpose |
|---|---|---|
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |
| Step 5 | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name***path-name* \| *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic bandwidth 500` | Adds a Path Option for Bandwidth Override to specify a bandwidth fallback for a path option for an MPLS TE tunnel.<br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name***path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br><br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br><br>• The **attributes***string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| Step 6 | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |

## Modifying the Bandwidth on a Path Option for Bandwidth Override

Perform this task to modify the bandwidth on a Path Option for Bandwidth Override. You might need to further reduce or modify the bandwidth constraint for a path option to ensure that the headend of a tunnel establishes an LSP.

The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. To force immediate reoptimization of all traffic engineering tunnels, you can use the

**mplstraffic-engreoptimize** command. You can also configure the **lockdown** command with bandwidth override to prevent automatic reoptimization.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name***path-name* | *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**
7. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type number*<br><br>**Example:**<br><br>`Router(config)# interface tunnel 1` | Configures the interface type and enters interface configuration mode.<br><br>• The *type* argument is the type of interface that you want to configure.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br><br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br><br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |

| | Command or Action | Purpose |
|---|---|---|
| Step 5 | **tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name***path-name* \| *path-number*} [**verbatim**]} [**attributes***string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500`<br><br>**Example:** | Adds a Path Option for Bandwidth Override to specify a bandwidth fallback for a path option for an MPLS TE tunnel.<br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name***path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br><br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br><br>• The **attributes***string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| Step 6 | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |
| Step 7 | **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]<br><br>**Example:**<br><br>`Router# show mpls traffic-eng tunnels tunnel1` | (Optional) Displays information about tunnels.<br>• Use the **showmplstraffic-engtunnels** command to verify which bandwidth path option is in use by the LSP. |

## Removing a Path Option for Bandwidth Override

Perform this task to remove the bandwidth on the path option for bandwidth override. The Path Option for Bandwidth Override feature is designed as a temporary reduction in bandwidth constraint. Use this task to remove the bandwidth override when it is not required.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel destination** {*hostname* | *ip-address*}
5. **no tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** | **global**] *kbps*] [**lockdown**]
6. **end**
7. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br>`Router(config)# interface tunnel 1` | Configures a tunnel interface type and enters interface configuration mode.<br>• The *number* argument is the number of the tunnel interface that you want to create or configure. |
| Step 4 | **tunnel destination** {*hostname* \| *ip-address*}<br><br>**Example:**<br>`Router(config-if)# tunnel destination 10.10.10.12` | Specifies the destination of the tunnel for this path option.<br>• The *hostname* argument is the name of the host destination.<br>• The *ip-address* argument is the IP address of the host destination expressed in decimal in four-part, dotted notation. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **no tunnel mpls traffic-eng path-option** *number* {**dynamic** \| **explicit** {**name** *path-name* \| *path-number*} [**verbatim**]} [**attributes** *string*] [**bandwidth** [**sub-pool** \| **global**] *kbps*] [**lockdown**]<br><br>**Example:**<br><br>`Router(config-if)# no tunnel mpls traffic-eng path-option 2 dynamic bandwidth 500` | Removes a path option for bandwidth override that specifies a bandwidth fallback for a path option for an MPLS TE tunnel.<br>• The *number* argument identifies the path option.<br>• The **dynamic** keyword indicates that the path option is dynamically calculated (the router figures out the best path).<br>• The **explicit** keyword indicates that the path option is specified. You specify the IP addresses of the path.<br>• The **name** *path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br>• The **attributes** *string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The **global** keyword indicates a global pool path option. Entering this keyword is not necessary, for all path options are from the global pool in the absence of the **sub-pool** keyword.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| **Step 6** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | (Optional) Exits to privileged EXEC mode. |
| **Step 7** | **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]<br><br>**Example:**<br><br>`Router# show mpls traffic-eng tunnels tunnel1` | (Optional) Displays information about tunnels.<br>• Use the **show mpls traffic-eng tunnels** command to verify which bandwidth path option is in use by the LSP. |

## Verifying that LSP Is Signaled Using the Correct Bandwidth

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]
3. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]

Use this command to verify that the LSP is signaled with the correct bandwidth and to verify that the bandwidth configured on the tunnel is overridden. For example:

**Example:**

```
Router# show mpls traffic-eng tunnels tunnel21
Name: Router-t21                      (Tunnel21) Destination: 10.10.10.12
  Status:
    Admin: up         Oper: up     Path: valid       Signalling: connected
    path option 2, type explicit path2 (Basis for Setup, path weight 65834)
    path option 1, type explicit path1
  Config Parameters:
    Bandwidth: 1000      kbps (Global)  Priority: 1  1   Affinity: 0x0/0xFFFF
    Metric Type: IGP (global)
    AutoRoute:  enabled   LockDown: disabled  Loadshare: 1        bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 2 is active
    BandwidthOverride: enabled   LockDown: disabled  Verbatim: disabled
    Bandwidth Override:
      Signalling: 500 kbps (Global)
      Overriding: 1000        kbps (Global) configured on tunnel
```

If bandwidth override is actively being signaled, the **show mpls traffic-eng tunnel** command displays the bandwidth override information under the Active Path Option Parameters heading. The example shows that BandwidthOverride is enabled and that the tunnel is signaled using path-option 2. The bandwidth signaled is 500. This is the value configured on the path option 2 and it overrides the 1000 kbps bandwidth configured on the tunnel interface.

**Step 3** **exit**

Use this command to exit to user EXEC mode. For example:

**Example:**

```
Router# exit
Router>
```

### Troubleshooting Tips

If the tunnel state is down and you configured a path-option with bandwidth override enabled, the **showmplstraffic-engtunnels** command indicates other reasons why a tunnel is not established. For example:

- The tunnel destination is not in the routing table.
- If the bandwidth override value is not zero, the bandwidth constraint may still be too large.
- Other attributes configured on the tunnel, such as affinity, might prevent the calculation of a path over the existing topology.
- TE might not be configured on all links necessary to reach tunnel destination.

# Configuration Examples for MPLS Traffic Engineering--RSVP Hello State Timer



## Configuring LSP Attribute List Examples



### Configuring an LSP Attribute List: Example

This example shows the configuration of the affinity, bandwidth, and priority LSP-related attributes in an LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
```

### Adding Attributes to an LSP Attribute List: Example

This example shows the addition of protection attributes to the LSP attribute list identified with the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# protection fast-reroute
Router(config-lsp-attr)# exit
```

## Removing an Attribute from an LSP Attribute List: Example

The following example shows removing the priority attribute from the LSP attribute list identified by the string simple:

```
Router(config)# mpls traffic-eng lsp attributes simple
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list
LIST simple
 priority 1 1
!
Router(config-lsp-attr)# no priority
Router(config-lsp-attr)# list
LIST simple
!
Router(config-lsp-attr)# exit
```

## Modifying an Attribute in an LSP Attribute List: Example

The following example shows modifying the bandwidth in an LSP attribute list identified by the numeral 5:

```
Router(config)# mpls traffic-eng lsp attributes 5
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# list
LIST 5
 bandwidth 1000
 priority 1 1
Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# list
LIST 5
 bandwidth 500
 priority 1 1
Router(config-lsp-attr)# exit
```

## Deleting an LSP Attribute List: Example

The following example shows the deletion of an LSP attribute list identified by numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1

Router(config-lsp-attr)# exit
!
Router(config)# no mpls traffic-eng lsp attributes 1
```

## Associating an LSP Attribute List with a Path Option for a TE Tunnel: Example

The following example associates the LSP attribute list identified by the numeral 3 with path option 1:

```
Router(config)# mpls traffic-eng lsp attributes 3
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 2 2
Router(config-lsp-attr)# protection fast-reroute
Router(config-lsp-attr)# exit
!
!
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered FastEthernet1/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 3
```

In this configuration, the LSP will have the following attributes:

```
{bandwidth = 1000
 priority = 2 2
 affinity 1
 reroute enabled.
 }
```

The LSP attribute list referenced by the path option will take precedence over the values configured on the tunnel interface.

## Modifying a Path Option to Use a Different LSP Attribute List: Example

The following example modifies path option 1 to use an LSP attribute list identified by the numeral 1:

```
Router(config)# mpls traffic-eng lsp attributes 1
Router(config-lsp-attr)# affinity 7 7
Router(config-lsp-attr)# bandwidth 500
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
Router(config)# mpls traffic-eng lsp attributes 2
Router(config-lsp-attr)# bandwidth 1000
Router(config-lsp-attr)# priority 1 1
Router(config-lsp-attr)# exit
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered FastEthernet1/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
Router(config-if)# tunnel mpls traffic-eng path-option 1 dynamic attributes 1
```

In this configuration, the LSP has the following attributes:

```
{affinity = 7 7
 bandwidth = 500
 priority = 1 1
 }
```

## Removing a Path Option for an LSP for an MPLS TE Tunnel: Example

The following example shows the removal of path option 1 for an LSP for a TE tunnel:

```
Router(config)# interface Tunnel 1
Router(config-if)# ip unnumbered FastEthernet1/0/1
Router(config-if)# tunnel destination 10.112.0.12
Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# tunnel mpls traffic-eng affinity 1
Router(config-if)# tunnel mpls traffic-eng bandwidth 5000
```

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
Router(config-if)# tunnel mpls traffic-eng path-option 2 explicit path2 attributes 2
!
!
Router(config-if)# no tunnel mpls traffic-eng path-option 1 explicit path1 attributes 1
```

# Configuring a Path Option for Bandwidth Override Examples



## Configuring a Path Option to Override the Bandwidth: Example

The following examples show how to configure a path option to override the bandwidth:

```
Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 ?
       attributes Specify an LSP attribute list
       bandwidth  override the bandwidth configured on the tunnel
       lockdown   not a candidate for reoptimization
       <cr>
Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth ?
       <0-4294967295>  bandwidth requirement in kbps
       sub-pool        tunnel uses sub-pool bandwidth
Router(config-if)# tunnel mpls traffic-eng path-option 3 explicit name path1 bandwidth
500 ?
       lockdown   not a candidate for reoptimization
       <cr>
```

**Note** Once you configure bandwidth as a path-option parameter, you can no longer configure an LSP attribute list as a path-option parameter.

## Example Configuring Fallback Bandwidth Path Options for TE Tunnels

The following example shows multiple path options configured with the **tunnel mpls traffic-eng path-option** command:

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
end
```

The device selects a path option for an LSP in order of preference, as follows:

- The device attempts to signal an LSP using path options starting with path-option 1.

The device attempts to signal an LSP with the 1000 kbps bandwidth configured on the tunnel interface because path-option 1 has no bandwidth configured.

- If 1000 kbps bandwidth is not available over the network, the device attempts to establish an LSP using path-option 2.

Path-option 2 has a bandwidth of 500 kbps configured. This reduces the bandwidth constraint from the original 1000 kbps configured on the tunnel interface.

- If 500 kbps is not available, the device attempts to establish an LSP using path-option 3.

Path-option 3 is configured as dynamic and has bandwidth 0. The device establishes the LSP if an IP path exists to the destination and all other tunnel constraints are met.

## Modifying the Bandwidth on a Path Option for Bandwidth Override: Example

The following example shows modifying the bandwidth on a path option for bandwidth override. Path-option 3 is changed to an explicit path with a bandwidth of 100 kbps. Path-option 4 is configured with bandwidth 0.

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 dynamic bandwidth 0
!
!
Router(config)# tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
Router(config)# tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
```

## Removing the Path Option Bandwidth Value for an LSP for an MPLS TE Tunnel: Example

The following example shows the removal of the bandwidth for path option 3 for an LSP for an MPLS TE tunnel:

```
interface Tunnel 1
 ip unnumbered Loopback0
 tunnel destination 10.10.10.12
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 1 explicit name path1
 tunnel mpls traffic-eng path-option 2 explicit name path2 bandwidth 500
 tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
 tunnel mpls traffic-eng path-option 4 dynamic bandwidth 0
!
Router(config)# no tunnel mpls traffic-eng path-option 3 explicit name path3 bandwidth 100
```

# Additional References

### Related Documents

| Related Topic | Document Title |
| --- | --- |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| MPLS TE command descriptions | *Cisco IOS Multiprotocol Label Switching Command Reference* |

### Standards

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

### MIBs

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

### RFCs

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

### Technical Assistance

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

# Feature Information for MPLS Traffic Engineering LSP Attributes

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 4 Feature Information for MPLS Traffic Engineering--LSP Attributes***

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering LSP Attributes | Cisco IOS XE Release 2.3 | This document describes how to configure label switched path (LSP) attributes for path options associated with Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels.<br><br>The MPLS Traffic Engineering--LSP Attributes feature is an extension to MPLS TE that provides an LSP Attribute List feature and a Path Option for Bandwidth Override feature. These features provide flexibility in the configuration of LSP attributes for MPLS TE tunnel path options. Several LSP attributes can be applied to path options for TE tunnels using an LSP attribute list. If bandwidth is the only LSP attribute you require, then you can configure a Path Option for Bandwidth Override.<br><br>In Cisco IOS XE Release 2.3, this feature was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.<br><br>The following sections provide information about this feature: |

| Feature Name | Releases | Feature Information |
|---|---|---|
| | | The following commands were introduced or modified: **affinity** (LSP Attributes), **auto-bw**(LSP Attributes), **bandwidth**(LSP Attributes), **exit**(LSP Attributes), **list**(LSP Attributes), **lockdown**(LSP Attributes), **mpls traffic-eng lsp attributes**, **priority**(LSP Attributes), **protection**(LSP Attributes), **record-route**(LSP Attributes), **show mpls traffic-eng lsp attributes**, and **show mpls traffic-eng tunnels**. |

# Glossary

**bandwidth** --The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.

**bandwidth reservation** --The process of assigning bandwidth to users and applications served by a network. This process involves assigning priority to different flows of traffic based on how critical and delay-sensitive they are. This makes the best use of available bandwidth, and if the network becomes congested, lower-priority traffic can be dropped. Sometimes called bandwidth allocation

**global pool** --The total bandwidth allocated to an Multiprotocol Label Switching (MPLS) traffic engineering link.

**label switched path (LSP) tunnel** --A configured connection between two routers, using label switching to carry the packets.

**LSR** --label switch router. A Multiprotocol Label Switching (MPLS) node that can forward native Layer 3 packets. The LSR forwards a packet based on the value of a label attached to the packet.

**MPLS TE** --Multiprotocol Label Switching (MPLS) traffic engineering (formerly known as “RRR” or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

**subpool** --The more restrictive bandwidth in an Multiprotocol Label Switching (MPLS) traffic engineering link. The subpool is a portion of the link's overall global pool bandwidth.

**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. The application of scientific principles and technology to measure, model, and control internet traffic in order to simultaneously optimize traffic performance and network resource utilization.

**traffic engineering tunnel** --A label-switched tunnel used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

**tunnel** --A secure communication path between two peers, such as two routers.

# MPLS Traffic Engineering Verbatim Path Support

The MPLS Traffic Engineering--Verbatim Path Support feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for traffic engineering (TE), thereby bypassing the topology database verification process.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering--Verbatim Path Support

- A Multiprotocol Label Switching (MPLS) TE tunnel must be configured globally.
- MPLS TE must be enabled on all links.

# Restrictions for MPLS Traffic Engineering Verbatim Path Support

- The **verbatim** keyword can be used only on a label-switched path (LSP) that is configured with the explicit path option.
- This release does not support reoptimization on the verbatim LSP.

# Information About MPLS Traffic Engineering--RSVP Hello State Timer



## MPLS TE Verbatim Path Support Overview

MPLS TE LSPs usually require that all the nodes in the network are TE aware, meaning they have IGP extensions to TE in place. However, some network administrators want the ability to build TE LSPs to traverse nodes that do not support IGP extensions to TE, but that do support RSVP extensions to TE.

Verbatim LSPs are helpful when all or some of the intermediate nodes in a network do not support IGP extensions for TE.

When this feature is enabled, the IP explicit path is not checked against the TE topology database. Because the TE topology database is not verified, a Path message with IP explicit path information is routed using the shortest path first (SPF) algorithm for IP routing.

# How to Configure MPLS Traffic Engineering--Verbatim Path Support



## Configuring MPLS Traffic Engineering--Verbatim Path Support

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip unnumbered loopback** *number*
5. **tunnel destination** {*host-name*| *ip-address*}
6. **tunnel mode mpls traffic-eng**
7. **tunnel mpls traffic-eng bandwidth** {**sub-pool** *kbps* | *kbps}*
8. **tunnel mpls traffic-eng autoroute announce**
9. **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]
10. **tunnel mpls traffic-eng path-option** *preference-number* {**dynamic** [**attributes** *string* | **bandwidth** {**sub-pool** *kbps* | *kbps*} **| lockdown | verbatim**] | **explicit**{**name** *path-name* | **identifier** *path-number* **}}**
11. **exit**
12. **exit**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface tunnel** *number*<br><br>**Example:**<br>`Router(config)# interface tunnel 1` | Configures a tunnel interface and enters interface configuration mode.<br>• The *number* argument identifies the tunnel number to be configured. |
| **Step 4** | **ip unnumbered loopback** *number*<br><br>**Example:**<br>`Router(config-if)`<br>`# ip unnumbered loopback 1` | Configures an unnumbered IP interface, which enables IP processing without an explicit address. A loopback interface is usually configured with the router ID.<br>**Note** An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link. |
| **Step 5** | **tunnel destination** {*host-name*\| *ip-address*}<br><br>**Example:**<br>`Router(config-if)# tunnel destination 10.100.100.100` | Specifies the destination for a tunnel.<br>• The *host-name* argument is the name of the host destination.<br>• The *ip-address* argument is the IP Version 4 address of the host destination expressed in decimal in four-part, dotted notation. |
| **Step 6** | **tunnel mode mpls traffic-eng**<br><br>**Example:**<br>`Router(config-if)# tunnel mode mpls traffic-eng` | Sets the tunnel encapsulation mode to MPLS traffic engineering. |
| **Step 7** | **tunnel mpls traffic-eng bandwidth** {**sub-pool** *kbps* \| *kbps}*<br><br>**Example:**<br>`Router(config-if)# tunnel mpls traffic-eng bandwidth 1000` | Configures the bandwidth required for an MPLS TE tunnel and assigns it either to the sub-pool or the global pool.<br>• The **sub-pool** keyword indicates a subpool tunnel.<br>• The *kbps* argument is the bandwidth, in kilobits per second, set aside for the MPLS TE tunnel. The range is from 1 to 4294967295. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **tunnel mpls traffic-eng autoroute announce**<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng autoroute announce` | Specifies that IGP should use the tunnel (if the tunnel is up) in its enhanced SPF calculation. |
| **Step 9** | **tunnel mpls traffic-eng priority** *setup-priority* [*hold-priority*]<br><br>**Example:**<br><br>`Router(config-if)# tunnel mpls traffic-eng priority 1 1` | Configures setup and reservation priority for a tunnel.<br>• The *setup-priority* argument is the priority used when signaling an LSP for this tunnel to determine which existing tunnels can be preempted.<br>Valid values are from 0 to 7. A lower number indicates a higher priority. An LSP with a setup priority of 0 can preempt any LSP with a non-0 priority.<br>• The *hold-priority* argument is the priority associated with an LSP for this tunnel to determine if it should be preempted by other LSPs that are being signaled.<br>Valid values are from 0 to 7, where a lower number indicates a higher priority. |

| | Command or Action | Purpose |
|---|---|---|
| Step 10 | **tunnel mpls traffic-eng path-option** *preference-number* {**dynamic** [**attributes** *string* \| **bandwidth** {**sub-pool** *kbps* \| *kbps*} \| **lockdown** \| **verbatim**] \| **explicit**{**name** *path-name* \| **identifier** *path-number* **}}**<br><br>**Example:**<br>`Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test verbatim`<br><br>**Example:** | Specifies LSP-related parameters, including the **verbatim** keyword used with an explicit path option, for an MPLS TE tunnel.<br>• The *preference-number* argument identifies the path option.<br>• The **protect** keyword and *preference-number argument identify the path option with protection.*<br>• The **dynamic** keyword indicates that the path option is dynamically calculated. (The router figures out the best path.)<br>• The **explicit** keyword indicates that the path option is specified. The IP addresses are specified for the path.<br>• The **name** *path-name*keyword argument combination identifies the name of the explicit path option.<br>• The *path-number* argument identifies the number of the explicit path option.<br>• The **verbatim** keyword bypasses the topology database verification.<br><br>**Note** You can use the **verbatim** keyword only with the explicit path option.<br><br>• The **attributes** *string* keyword argument combination names an attribute list to specify path options for the LSP.<br>• The **bandwidth** keyword specifies the LSP bandwidth.<br>• The **sub-pool** keyword indicates a subpool path option.<br>• The *kbps* argument is the number of kilobits per second set aside for the path option. The range is from 1 to 4294967295.<br>• The **lockdown** keyword disables reoptimization of the LSP. |
| Step 11 | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| Step 12 | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Verifying Verbatim LSPs for MPLS TE Tunnels

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]
3. **disable**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **show mpls traffic-eng tunnels** *tunnel-interface* [**brief**]<br><br>**Example:**<br><br>`Router# show mpls traffic-eng tunnels tunnel1` | Displays information about tunnels including those configured with an explicit path option using verbatim. |
| Step 3 | **disable**<br><br>**Example:**<br><br>`Router# disable` | (Optional) Exits to user EXEC mode. |

# Configuration Example for MPLS Traffic Engineering Verbatim Path Support

• Configuring MPLS Traffic Engineering Verbatim Path Support Example, page 115

## Configuring MPLS Traffic Engineering Verbatim Path Support Example

The following example shows a tunnel that has been configured with an explicit path option using verbatim:

```
interface tunnel 1
 ip unnumbered loopback 1
 tunnel destination 10.10.100.100
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng path-option 1 explicit name path1 verbatim
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| MPLS commands | *Cisco IOS Multiprotocol Label Switching Command Reference* |
| Interface commands | *Cisco IOS Interface and Hardware Component Command Reference* |

### Standards

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

### MIBs

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

### RFCs

| RFC | Title |
|---|---|
| No new or modified RFCs are supported by this release. | -- |

### Technical Assistance

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

# Feature Information for MPLS Traffic Engineering Verbatim Path Support

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 5 Feature Information for MPLS Traffic Engineering Verbatim Path Support*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering--Verbatim Path Support | Cisco IOS XE Release 2.3 | The MPLS Traffic Engineering Verbatim Path Support feature allows network nodes to support Resource Reservation Protocol (RSVP) extensions without supporting Interior Gateway Protocol (IGP) extensions for traffic engineering (TE), thereby bypassing the topology database verification process.<br>This feature was integrated into Cisco IOS XE Release 2.3.<br>The following commands were introduced or modified: **show mpls traffic-eng tunnels**, **tunnel mpls traffic-eng path option**. |

# Glossary

**Fast Reroute** --Procedures that enable temporary routing around a failed link or node while a new label-switched path (LSP) is being established at the head end.

**headend** --The router that originates and maintains a given label-switched path (LSP) . This is the first router in the LSP’s path.

**IGP** --Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information protocol (RIP).

**LSP** --label-switched path. A configured connection between two routers, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

**LSR** --label switching router. A device that forwards Multiprotocol Label Switching (MPLS) packets based on the value of a fixed-length label encapsulated in each packet.

**merge point** --The backup tunnel’s tail.

**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 (frames). ATM switches or existing routers in the network core can switch packets according to the labels with minimal lookup overhead.

**PLR** --point of local repair. The head-end of the backup tunnel.

**RSVP** --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

**SPF** --shortest path first. Routing algorithm that iterates on length of path to determine a shortest-path spanning tree. Commonly used in link-state routing algorithms. Sometimes called Dijkstra's algorithm.

**tailend** --The router upon which an label-switched path (LSP) is terminated. This is the last router in the LSP's path.

**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 communications path between two peers, such as routers.

# MPLS Traffic Engineering--RSVP Hello State Timer

The MPLS Traffic Engineering--RSVP Hello State Timer feature detects when a neighbor is down and quickly triggers a state timeout, which frees resources such as bandwidth that can be reused by other label switched paths (LSPs).

Resource Reservation Protocol (RSVP) hellos can be used to detect when a neighboring node is down. The hello state timer then triggers a state timeout. As a result, network convergence time is reduced, and nodes can forward traffic on alternate paths or assist in stateful switchover (SSO) operation.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering--RSVP Hello State Timer

Perform the following tasks on routers before configuring the MPLS Traffic Engineering--RSVP Hello State Timer feature:

- Configure Resource Reservation Protocol (RSVP).

- Enable Multiprotocol Label Switching (MPLS).
- Configure traffic engineering (TE).
- Enable hellos for state timeout.

# Restrictions for MPLS Traffic Engineering--RSVP Hello State Timer

- Hellos for state timeout are dependent on graceful restart, if it is configured; however, graceful restart is independent of hellos for state timeout.
- Unnumbered interfaces are not supported.
- Hellos for state timeout are configured on a per-interface basis.

# Information About MPLS Traffic Engineering--RSVP Hello State Timer



## Hellos for State Timeout

When RSVP signals a TE LSP and there is a failure somewhere along the path, the failure can remain undetected for as long as two minutes. During this time, bandwidth is held by the nonfunctioning LSP on the nodes downstream from the point of failure along the path with the state intact. If this bandwidth is needed by headend tunnels to signal or resignal LSPs, tunnels may fail to come up for several minutes thereby negatively affecting convergence time.

Hellos enable RSVP nodes to detect when a neighboring node is not reachable. After a certain number of intervals, hellos notice that a neighbor is not responding and delete its state. This action frees the node's resources to be reused by other LSPs.

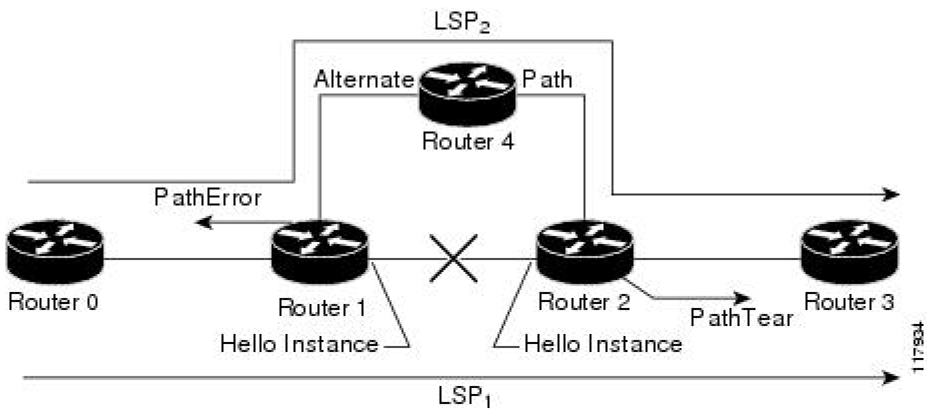
Hellos must be configured both globally on the router and on the specific interface to be operational.

## Hello Instance

A hello instance implements RSVP hellos for a given router interface address and a remote IP address. A hello instance is expensive because of the large number of hello requests that are sent and the strains they put on the router resources. Therefore, you should create a hello instance only when it is needed to time out state and delete the hello instance when it is no longer necessary.

## Hellos for Nonfast-Reroutable TE LSP

The figure below shows a nonfast-reroutable TE LSP from Router 1 to Router 3 via Router 2.




Assume that the link between Router 1 and Router 2 fails. This type of problem can be detected by various means including interface failure, Interior Gateway Protocol (IGP) (Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS)), and RSVP hellos. However, sometimes interface failure cannot be detected; for example, when Router 1 and Router 2 are interconnected through a Layer 2 switch. The IGP may be slow detecting the failure. Or there may be no IGP running between Router 1 and Router 2; for example, between two Autonomous System Boundary Routers (ASBRs) interconnecting two autonomous systems.

If hellos were running between Router 1 and Router 2, each router would notice that communication was lost and time out the state immediately.

Router 2 sends a delayed PathTear message to Router 3 so that the state can be deleted on all nodes thereby speeding up the convergence time.

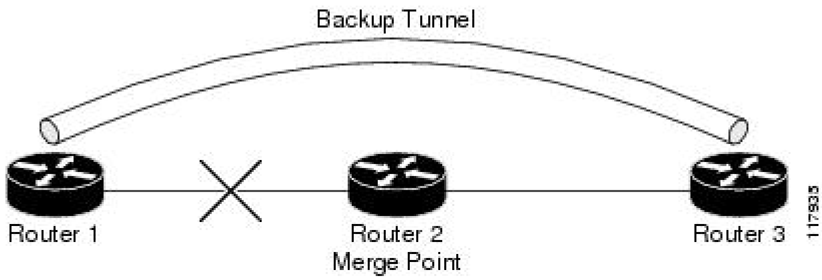
**Note** The PathTear message is delayed one second because on some platforms data is being forwarded even after the control plane is down.

Router 1 sends a destructive PathError message upstream to Router 0 with error code ROUTING_PROBLEM and error value NO_ROUTE.

LSP1 goes from Router 0 to Router 1 to Router 2 to Router 3; LSP 2 goes from Router 0 to Router 1 to Router 4 to Router 2 to Router 3.

# Hellos for Fast-Reroutable TE LSP with Backup Tunnel

The figure below shows a fast reroutable TE LSP with a backup tunnel from Router1 to Router 2 to Router 3.




This TE LSP has a backup tunnel from Router 1 to Router 3 protecting the fast reroutable TE LSP against a failure in the Router 1 to Router 2 link and node Router 2. However, assume that a failure occurs in the link connecting Router 1 to Router 2. If hellos were running between Router 1 and Router 2, the routers would notice that the link is down, but would not time out the state. Router 2 notices the failure, but cannot time out the TE LSP because Router 2 may be a merge point, or another downstream node may be a merge point. Router 1 notices the failure and switches to the backup LSP; however, Router 1 cannot time out the state either.

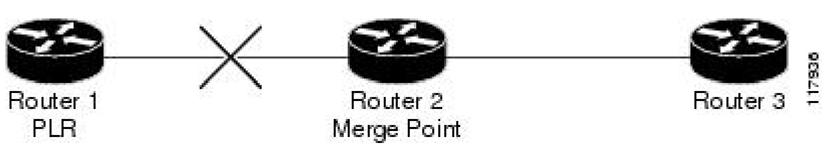
**Note** A hello instance is not created in the preceding scenario because the neighbor is down and the hello instance cannot take action.

# Hellos for Fast-Reroutable TE LSP Without Backup Tunnel

On a fast-reroutable TE LSP with no backup tunnel, a hello instance can be created with the neighbor downstream (next hop (NHOP)). On a nonfast-reroutable TE LSP, a hello instance can be created with the neighbor downstream (NHOP) and the neighbor upstream (previous hop (PHOP)). This is in addition to the existing hellos for Fast Reroute.

**Note** If both Fast Reroute and hellos for state timeout hello instances are needed on the same link, only one hello instance is created. It will have the Fast Reroute configuration including interval, missed refreshes, and differentiated services code point (DSCP). When a neighbor is down, Fast Reroute and the hello state timer take action.

The figure below shows a fast-reroutable TE LSP. without a backup tunnel, from Router 1 (the point of local repair (PLR)), to Router 2 to Router 3.




Assume that a failure occurs in the link connecting Router 1 to Router 3. Router 1 can time out the state for the TE LSP because Router 1 knows there is no backup tunnel. However, Router 2 cannot time out the state because Router 2 does not know whether a backup tunnel exists. Also, Router 2 may be a merge point, and therefore cannot time out the state.

**Note** A hello instance is not created in the preceding scenario because the neighbor is down and the hello instance cannot take action.

# How to Configure MPLS Traffic Engineering--RSVP Hello State Timer

**Note** The following tasks also enable Fast Reroute; however, this section focuses on the RSVP hello state timer.



## Enabling the Hello State Timer Globally

Perform this task to enable the RSVP hello state timer globally to reduce network convergence, allow nodes to forward traffic on alternate paths, or assist in stateful switchover (SSO) operation.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling hello**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **ip rsvp signalling hello**<br><br>**Example:**<br><br>`Router(config)#` **ip rsvp signalling hello** | Enables hellos for state timeout globally on a router. |
| Step 4 | **end**<br><br>**Example:**<br><br>`Router(config)# end` | Exits to privileged EXEC mode. |

# Enabling the Hello State Timer on an Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **ip rsvp signalling hello**
5. **end**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br><br>`Router(config)# interface FastEthernet 0/0/0` | Enters interface configuration mode.<br><br>• The *type slot subslot* / *port*[**.** *subinterface-number*] arguments identify the interface to be configured. |
| **Step 4** | **ip rsvp signalling hello**<br><br>**Example:**<br><br>`Router(config-if)#` **ip rsvp signalling hello** | Enables hellos for state timeout on an interface. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Setting a DSCP Value on an Interface

Perform this task to set a differentiated services code point DSCP value for hello messages on an interface.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **ip rsvp signalling hello reroute dscp** *num*
5. **end**

## DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br>`Router(config)# interface FastEthernet 0/0/0` | Enters interface configuration mode.<br>• The *type slot* / *subslot* / *port*[**.** *subinterface-number*] arguments identify the interface to be configured. |
| **Step 4** | **ip rsvp signalling hello reroute dscp** *num*<br><br>**Example:**<br>`Router(config-if)# ip rsvp signalling hello reroute dscp 30` | Sets a DSCP value for RSVP hello messages on an interface of a router from 0 to 63 with hellos for state timeout enabled. |
| **Step 5** | **end**<br><br>**Example:**<br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Setting a Hello Request Interval on an Interface

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **ip rsvp signalling hello reroute refresh interval** *interval-value*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br><br>`Router(config)# interface FastEthernet 0/0/0` | Enters interface configuration mode.<br><br>• The *type slot subslot* / *port*[**.** *subinterface-number*] argument identifies the interface to be configured. |
| Step 4 | **ip rsvp signalling hello reroute refresh interval** *interval-value*<br><br>**Example:**<br><br>`Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000` | Sets a hello request interval on an interface of a router with hellos for state timer enabled. |
| Step 5 | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Setting the Number of Hello Messages that can be Missed on an Interface

Perform this task to set the number of consecutive hello messages that are lost (missed) before hello declares the neighbor down.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]
4. **ip rsvp signalling hello reroute refresh misses** *msg-count*
5. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| Step 2 | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface** *type slot* / *subslot* / *port* [**.** *subinterface-number*]<br><br>**Example:**<br><br>`Router(config)# interface FastEthernet 0/0/0` | Enters interface configuration mode.<br><br>• The *type slot subslot* / *port*[**.** *subinterface-number*] arguments identify the interface to be configured. |
| Step 4 | **ip rsvp signalling hello reroute refresh misses** *msg-count*<br><br>**Example:**<br><br>`Router(config-if)#` **ip rsvp signalling hello reroute refresh misses** *5* | Configures the number of consecutive hello messages that are lost before hello declares the neighbor down. |
| Step 5 | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | Exits to privileged EXEC mode. |

# Verifying Hello for State Timer Configuration

### SUMMARY STEPS

1. **enable**
2. **show ip rsvp hello**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br><br>`Router> enable` | (Optional) Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| Step 2 | **show ip rsvp hello**<br><br>**Example:**<br><br>`Router# show` **ip rsvp hello** | Displays the status of RSVP TE hellos and statistics including hello state timer (reroute). |

# Configuration Examples for MPLS Traffic Engineering--RSVP Hello State Timer



## Example

In the following example, the hello state timer is enabled globally and on an interface. Related parameters, including a DSCP value, a refresh interval, and a missed refresh limit, are set on an interface.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling hello
Router(config)# interface FastEthernet 0/0/0
Router(config-if)# ip rsvp signalling hello
Router(config-if)# ip rsvp signalling hello reroute dscp 30
Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000
Router(config-if)# ip rsvp signalling hello reroute refresh misses 5
Router(config-if)# end
```

The following example verifies the status of the hello state timer (reroute):

```
Router# show ip rsvp hello
Hello:
  Fast-Reroute/Reroute:Enabled
    Statistics:Enabled
  Graceful Restart:Enabled (help-neighbor only)
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples | • *Cisco IOS Quality of Service Solutions Command Reference*<br>• *Cisco IOS Multiprotocol Label Switching Command Reference* |
| Stateful Switchover | Stateful Switchover |
| MPLS Label Distribution Protocol | MPLS Label Distribution Protocol (LDP) Overview |
| Cisco nonstop forwarding | Cisco Nonstop Forwarding |
| Information on backup tunnels, link and node failures, RSVP hellos | MPLS TE: Link and Node Protection, with RSVP Hellos Support (with Fast Tunnel Interface Down Detection) |
| Graceful restart | NSF/SSO - MPLS TE and RSVP Graceful Restart |

### Standards

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

### MIBs

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

### RFCs

| RFC | Title |
|---|---|
| RFC 3209 | RSVP-TE: Extensions to RSVP for LSP Tunnels |

**Technical Assistance**

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

# Feature Information for MPLS Traffic Engineering--RSVP Hello State Timer

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 6 Feature Information for MPLS Traffic Engineering--RSVP Hello State Timer*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering--RSVP Hello State Timer | Cisco IOS XE Release 2.3 | The MPLS Traffic Engineering--RSVP Hello State Timer feature detects when a neighbor is down and quickly triggers a state timeout, which frees resources such as bandwidth that can be reused by other label switched paths (LSPs).<br>This feature was integrated into Cisco IOS XE Release 2.3.<br>The following commands were introduced or modified: **ip rsvp signalling hello dscp**, **ip rsvp signalling hello refresh interval**, **ip rsvp signalling hello refresh misses**, **ip rsvp signalling hello reroute dscp**, **ip rsvp signalling hello reroute refresh interval**, **ip rsvp signalling hello reroute refresh misses**, **show ip rsvp hello**. |

# Glossary

**autonomous system** --A collection of networks that share the same routing protocol and that are under the same system administration.

**ASBR** --autonomous system boundary router. A router that connects and exchanges information between two or more autonomous systems.

**backup tunnel** --A Multiprotocol Label Switching (MPLS) traffic engineering tunnel used to protect other (primary) tunnel traffic when a link or node failure occurs.

**DSCP** --differentiated services code point. Six bits in the IP header, as defined by the Internet Engineering Task Force (IETF). These bits determine the class of service provided to the IP packet.

**FRR** --Fast Reroute. A mechanism for protecting Multiprotocol Label Switching (MPLS) traffic engineering (TE) label switched paths (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.

**graceful restart** --A process for helping a neighboring Route Processor (RP) restart after a node failure has occurred.

**headend** --The router that originates and maintains a given label switched paths (LSP). This is the first router in the LSP’s path.

**IGP** --Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common Internet IGPs include Internal Gateway Routing Protocol (IGRP), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

**IS-IS** --Intermediate System-to-Intermediate System. Open systems Interconnection (OSI) link-state hierarchical routing protocol whereby Intermediate System (IS) routers exchange routing information based on a single metric to determine network topology.

**instance** --A mechanism that implements the RSVP hello extensions for a given router interface address and remote IP address. Active hello instances periodically send Hello Request messages, expecting Hello ACK messages in response. If the expected ACK message is not received, the active hello instance declares that the neighbor (remote IP address) is unreachable (that is, it is lost). This can cause LSPs crossing this neighbor to be fast rerouted.

**label** --A short, fixed-length data identifier that tells switching nodes how to forward data (packets or cells).

**LDP** --Label Distribution Protocol. The protocol that supports Multiprotocol Label Switching (MPLS) hop-by-hop forwarding by distributing bindings between labels and network prefixes. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

**LSP** --label switched path is a configured connection between two routers, in which Multiprotocol Label Switching (MPLS) is used to carry packets. The LSP is created by the concatenation of one or more label-switched hops, allowing a packet to be forwarded by swapping labels from one MPLS node to another MPLS node.

**merge point** --The backup tunnel’s tail.

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

**OSPF** --Open Shortest Path First. A link-state routing protocol used for routing.

**PLR** --point of local repair. The headend of the backup tunnel.

**RSVP** --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

**state** --Information that a router must maintain about each LSP. The information is used for rerouting tunnels.

**tailend** --The router upon which an LSP is terminated. This is the last router in the LSP’s path.

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

**topology** --The physical arrangement of network nodes and media within an enterprise networking structure.

**tunnel** --Secure communications path between two peers, such as two routers.

# MPLS Traffic Engineering Forwarding Adjacency

The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a traffic engineering (TE) label switched path (LSP) tunnel as a link in an Interior Gateway Protocol (IGP) network based on the Shortest Path First (SPF) algorithm.

Both Intermediate System-to-Intermediate System (IS-IS) and Open Shortest Path First (OSPF) are supported.



## Finding Feature Information

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

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

## Prerequisites for MPLS Traffic Engineering Forwarding Adjacency

Your network must support the following Cisco IOS XE features:

- Multiprotocol Label Switching (MPLS)
- IP Cisco Express Forwarding
- IS-IS

# Restrictions for MPLS Traffic Engineering Forwarding Adjacency

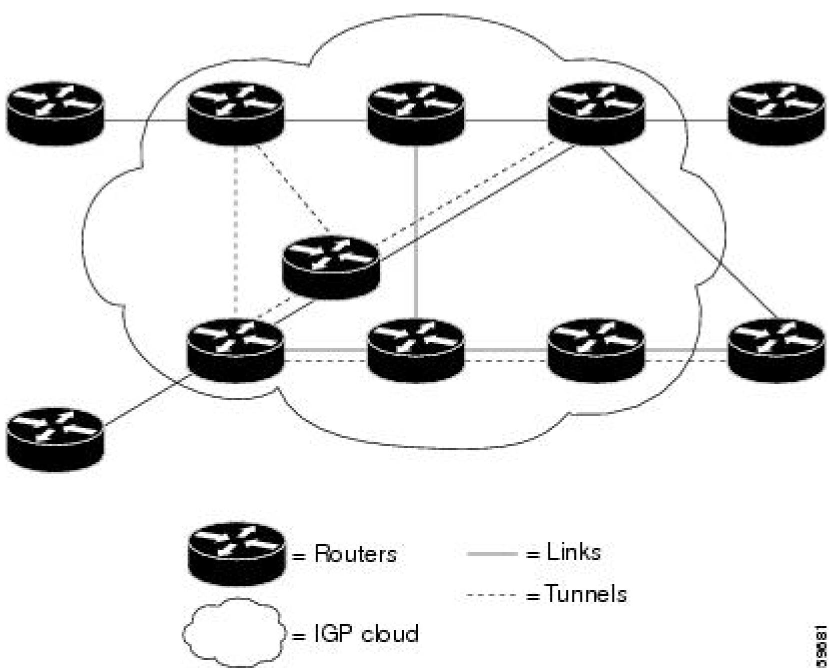
- Using the MPLS Traffic Engineering Forwarding Adjacency feature increases the size of the IGP database by advertising a TE tunnel as a link.
- When the MPLS Traffic Engineering Forwarding Adjacency feature is enabled on a TE tunnel, the link is advertised in the IGP network as a type, length, value (TLV) 22 object without any TE sub-TLV.
- You must configure MPLS TE forwarding adjacency tunnels bidirectionally.

# Information About MPLS Traffic Engineering Forwarding Adjacency



## MPLS Traffic Engineering Forwarding Adjacency Functionality

The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a TE LSP tunnel as a link in an IGP network based on the SPF algorithm. A forwarding adjacency can be created between routers regardless of their location in the network. The routers can be located multiple hops from each other, as shown in the figure below.



As a result, a TE tunnel is advertised as a link in an IGP network with the link's cost associated with it.

Routers outside of the TE domain see the TE tunnel and use it to compute the shortest path for routing traffic throughout the network.

## MPLS Traffic Engineering Forwarding Adjacency Benefits

TE tunnel interfaces advertised for SPF--TE tunnel interfaces are advertised in the IGP network just like any other links. Routers can then use these advertisements in their IGPs to compute the SPF even if they are not the headend of any TE tunnels.

# How to Configure MPLS Traffic Engineering Forwarding Adjacency

- Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency, page 137
- Configuring MPLS TE Forwarding Adjacency on Tunnels, page 138
- Verifying MPLS TE Forwarding Adjacency, page 139

## Configuring a Tunnel Interface for MPLS TE Forwarding Adjacency

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **exit**
5. **exit**

### DETAILED STEPS

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

| | Command or Action | Purpose |
|---|---|---|
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br>`Router(config)# interface tunnel 0` | Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode. |
| Step 4 | **exit**<br><br>**Example:**<br>`Router(config-if)# exit` | Exits interface configuration mode and returns to global configuration mode. |
| Step 5 | **exit**<br><br>**Example:**<br>`Router(config)# exit` | Exits global configuration mode and returns to privileged EXEC mode. |

# Configuring MPLS TE Forwarding Adjacency on Tunnels

**Note** You must configure a forwarding adjacency on two LSP tunnels bidirectionally, from A to B and B to A. Otherwise, the forwarding adjacency is advertised, but not used in the IGP network.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **tunnel mpls traffic-eng forwarding-adjacency** [**holdtime** *value*]
5. **isis metric** {*metric-value*| **maximum**} {**level-1**| **level-2**}

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| Step 1 | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| Step 2 | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| Step 3 | **interface tunnel** *number*<br><br>**Example:**<br>`Router(config)# interface tunnel 0` | Designates a tunnel interface for the forwarding adjacency, and enters interface configuration mode. |
| Step 4 | **tunnel mpls traffic-eng forwarding-adjacency** [**holdtime** *value*]<br><br>**Example:**<br>`Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency` | Advertises a TE tunnel as a link in an IGP network. |
| Step 5 | **isis metric** {*metric-value*\| **maximum**} {**level-1**\| **level-2**}<br><br>**Example:**<br>`Router(config-if)# isis metric 2 level-1` | Configures the IS-IS metric for a tunnel interface to be used as a forwarding adjacency.<br>• You should specify the **isis metric** command with level-1 or level-2 to be consistent with the IGP level at which you are performing traffic engineering. Otherwise, the metric has the default value of 10. |

# Verifying MPLS TE Forwarding Adjacency

### SUMMARY STEPS

1. **enable**
2. **show mpls traffic-eng forwarding-adjacency** [*ip-address*]
3. **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]
4. **exit**

### DETAILED STEPS

**Step 1** **enable**

Use this command to enable privileged EXEC mode. Enter your password if prompted. For example:

**Example:**

```
Router> enable
Router#
```

**Step 2** **show mpls traffic-eng forwarding-adjacency** [*ip-address*]

Use this command to see the current tunnels. For example:

**Example:**

```
Router# show mpls traffic-eng forwarding-adjacency

 destination 0168.0001.0007.00 has 1 tunnels
  Tunnel7     (traffic share 100000, nexthop 192.168.1.7)
                (flags:Announce Forward-Adjacency, holdtime 0)
Router# show mpls traffic-eng forwarding-adjacency 192.168.1.7
 destination 0168.0001.0007.00 has 1 tunnels
  Tunnel7     (traffic share 100000, nexthop 192.168.1.7)
                (flags:Announce Forward-Adjacency, holdtime 0)
```

**Step 3** **show isis** [*process-tag*] **database** [**level-1**] [**level-2**] [**l1**] [**l2**] [**detail**] [**lspid**]

Use this command to display information about the IS-IS link-state database. For example:

**Example:**

```
Router# show isis database
IS-IS Level-1 Link State Database

LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.00-00  0x0000000C     0x5696        792           0/0/0
0000.0C00.40AF.00-00  0x00000009     0x8452        1077          1/0/0
0000.0C00.62E6.00-00  0x0000000A     0x38E7        383           0/0/0
0000.0C00.62E6.03-00  0x00000006     0x82BC        384           0/0/0
0800.2B16.24EA.00-00  0x00001D9F     0x8864        1188          1/0/0
0800.2B16.24EA.01-00  0x00001E36     0x0935        1198          1/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num    LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0C00.0C35.03-00  0x00000005     0x04C8        792           0/0/0
0000.0C00.3E51.00-00  0x00000007     0xAF96        758           0/0/0
0000.0C00.40AF.00-00  0x0000000A     0x3AA9        1077          0/0/0
```

**Step 4** **exit**

Use this command to exit to user EXEC. For example:

**Example:**

```
Router# exit
Router>
```

# Configuration Examples for MPLS Traffic Engineering Forwarding Adjacency

This section provides a configuration example for the MPLS Traffic Engineering Forwarding Adjacency feature using an IS-IS metric.

- Example MPLS TE Forwarding Adjacency, page 141
- Usage Tips, page 142

# Example MPLS TE Forwarding Adjacency

The following output shows the configuration of a tunnel interface, a forwarding adjacency, and an IS-IS metric:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface tunnel 7
Router(config-if)# tunnel mpls traffic-eng forwarding-adjacency
Router(config-if)# isis metric 2 level-1
```

Following is sample command output when a forwarding adjacency has been configured:

```
Router# show running-config
Building configuration...
Current configuration :364 bytes
!
interface Tunnel7
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 192.168.1.7
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency
 tunnel mpls traffic-eng priority 7 7
 tunnel mpls traffic-eng path-option 10 explicit name short
 isis metric 2 level 1
```

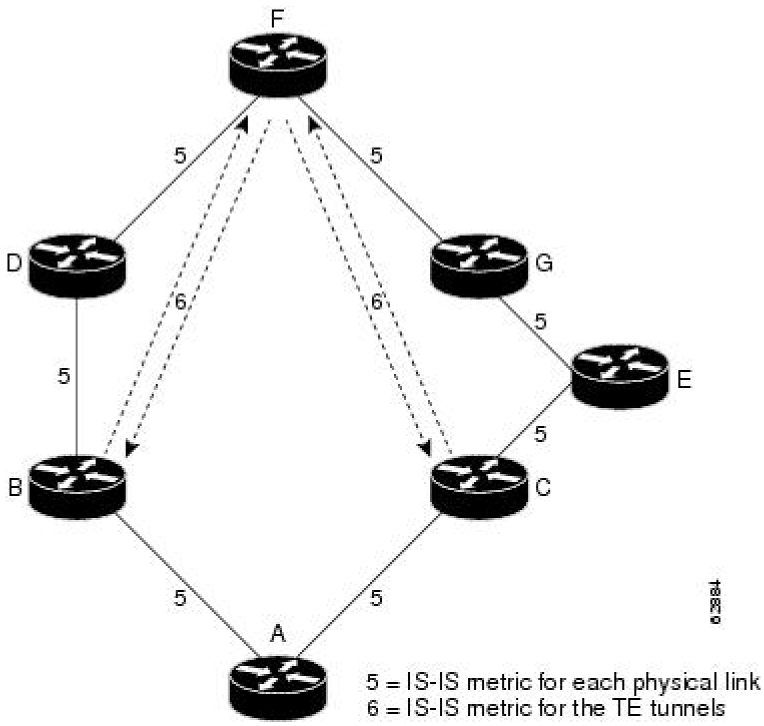
**Note** Do not specify the **tunnel mpls traffic-eng autoroute announce** command in your configuration when you are using forwarding adjacency.

Following is an example where forwarding adjacency is configured with OFPF:

```
Router# configure terminal

Router# show running-config

Building configuration...
Current configuration : 310 bytes
interface tunnel 1
!
interface Tunnel1
 ip unnumbered Loopback0
 ip ospf cost 6
 tunnel destination 172.16.255.5
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng forwarding-adjacency  tunnel mpls
 traffic-eng priority 7 7
 tunnel mpls traffic-eng bandwidth 1000
 tunnel mpls traffic-eng path-option 10 dynamic
 end
Router# show mpls traffic-eng forwarding-adjacency

 destination 172.16.255.5, area ospf 172  area 0, has 1 tunnels
  Tunnel1      (load balancing metric 2000000, nexthop 172.16.255.5)
               (flags:  Forward-Adjacency, holdtime 0)
Router#
```

# Usage Tips

In the figure below, if you have no forwarding adjacencies configured for the TE tunnels between Band F and C and F, all the traffic that A must forward to F goes through B because B is the shortest path from A to F. (The cost from A to F is 15 through B and 20 through C.)




If you have forwarding adjacencies configured on the TE tunnels between B and F and C and F and also on the TE tunnels between F and B and F and C, then when A computes the SPF algorithm, A sees two equal cost paths of 11 to F. As a result, traffic across the A-B and A-C links is shared.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| MPLS traffic engineering commands | *Cisco IOS Multiprotocol Label Switching Command Reference* |
| IP switching commands | *Cisco IOS IP Switching Command Reference* |
| IS-IS TLVs | Intermediate System-to-Intermediate System (IS-IS) TLVs (white paper) |

### 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 standards has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

### RFCs

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

### Technical Assistance

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

# Glossary

**Cisco Express Forwarding** --A scalable, distributed, Layer 3 switching solution designed to meet the future performance requirements of the Internet and enterprise networks.

**forwarding adjacency** --A traffic engineering link (or LSP) into an IS-IS/OSPF network.

**IGP** --Interior Gateway Protocol. Internet protocol used to exchange routing information within an autonomous system. Examples of common IGPs include Interior Gateway Routing Protocol (IGRP), Open Shortest Path First ( OSPF), and Routing Information Protocol (RIP).

**IS-IS** --Intermediate System-to-Intermediate System. Open System Interconnection (OSI) link-state hierarchical routing protocol whereby Intermediate System (IS) routers exchange routing information based on a single metric to determine network topology.

**label switched path (LSP)** --A sequence of hops (R0...R*n* ) in which a packet travels from R0 to R*n* through label switching mechanisms. A switched path can be chosen dynamically, based on normal routing mechanisms, or through configuration.

**label switched path (LSP) tunnel** --A configured connection between two routers, using label switching to carry the packets.

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

**OSPF** --Open Shortest Path First. A link-state, hierarchical IGP routing algorithm proposed as a successor to RIP in the Internet community. OSPF features include least-cost routing, multipath routing, and load balancing. OSPF was derived from an early version of the IS-IS protocol. *See also* IS-IS.

**SPF** --Shortest Path First. A routing algorithm used as the basis for OSPF operations. When an SPF router is powered up, it initializes its routing-protocol data structures and then waits for indications from lower-layer protocols that its interfaces are functional.

**TLV** --type, length, value. A block of information embedded in Cisco Discovery Protocol advertisements.

**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 applied.

**traffic engineering tunnel** --A label switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing would cause the tunnel to take.

# Feature Information for MPLS Traffic Engineering Forwarding Adjacency

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 7 Feature Information for MPLS Traffic Engineering Forwarding Adjacency*

| Feature Name | Releases | Feature Information |
|---|---|---|
| MPLS Traffic Engineering Forwarding Adjacency | 12.0(15)S<br>12.0(16)ST<br>12.2(18)S<br>12.2(18)SXD<br>12.2(27)SBC<br>12.2(28)SB<br>12.4(20)T<br>Cisco IOS XE Release 2.3 | The MPLS Traffic Engineering Forwarding Adjacency feature allows a network administrator to handle a TE LSP tunnel as a link in an IGP network based on the SPF algorithm.<br>In 12.0(15)S, this feature was introduced.<br>In 12.0(16)ST, this feature was integrated.<br>In 12.2(18)S, this feature was integrated.<br>In 12.2(18)SXD, this feature was integrated.<br>In 12.2(27)SBC, this feature was integrated.<br>In 12.2(28)SB, this feature was integrated.<br>In 12.4(20)T, this feature was integrated.<br>In Cisco IOS XE Release 2.3, this feature was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.<br>The following commands were modified: **debug mpls traffic-eng forwarding-adjacency**, **show mpls traffic-eng forwarding-adjacency**, and **tunnel mpls traffic-eng forwarding-adjacency**. |

# RSVP Refresh Reduction and Reliable Messaging

The RSVP Refresh Reduction and Reliable Messaging feature includes refresh reduction, which improves the scalability, latency, and reliability of Resource Reservation Protocol (RSVP) signaling to enhance network performance and message delivery.

### History for the RSVP Refresh Reduction and Reliable Messaging Feature

| Release | Modification |
|---|---|
| 12.2(13)T | This feature was introduced. |
| 12.0(24)S | This feature was integrated into Cisco IOS Release 12.0(24)S. |
| 12.2(14)S | This feature was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(26)S | Two commands, **ip rsvp signalling refresh misses**and **ip rsvp signalling refresh interval**, were added into Cisco IOS Release 12.0(26)S. |
| 12.0(29)S | The *burst* and *max-size* argument defaults for the **ip rsvp signalling rate-limit** command were increased to 8 messages and 2000 bytes, respectively. |
| 12.2(28)SB | This feature was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(18)SXF5 | This feature was integrated into Cisco IOS Release 12.2(18)SXF5. |
| 12.2(33)SRB | This feature was integrated into Cisco IOS Release 12.2(33)SRB. |

### Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

# Finding Feature Information

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

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

# Prerequisites for RSVP Refresh Reduction and Reliable Messaging

RSVP must be configured on two or more routers within the network before you can use the RSVP Refresh Reduction and Reliable Messaging feature.

# Restrictions for RSVP Refresh Reduction and Reliable Messaging

Multicast flows are not supported for the reliable messages and summary refresh features.

# Information About RSVP Refresh Reduction and Reliable Messaging



## Feature Design of RSVP Refresh Reduction and Reliable Messaging

RSVP is a network-control, soft-state protocol that enables Internet applications to obtain special qualities of service (QoS) for their data flows. As a soft-state protocol, RSVP requires that state be periodically refreshed. If refresh messages are not transmitted during a specified interval, RSVP state automatically times out and is deleted.

In a network that uses RSVP signaling, reliability and latency problems occur when an RSVP message is lost in transmission. A lost RSVP setup message can cause a delayed or failed reservation; a lost RSVP refresh message can cause a delay in the modification of a reservation or in a reservation timeout. Intolerant applications can fail as a result.

Reliability problems can also occur when there is excessive RSVP refresh message traffic caused by a large number of reservations in the network. Using summary refresh messages can improve reliability by significantly reducing the amount of RSVP refresh traffic.

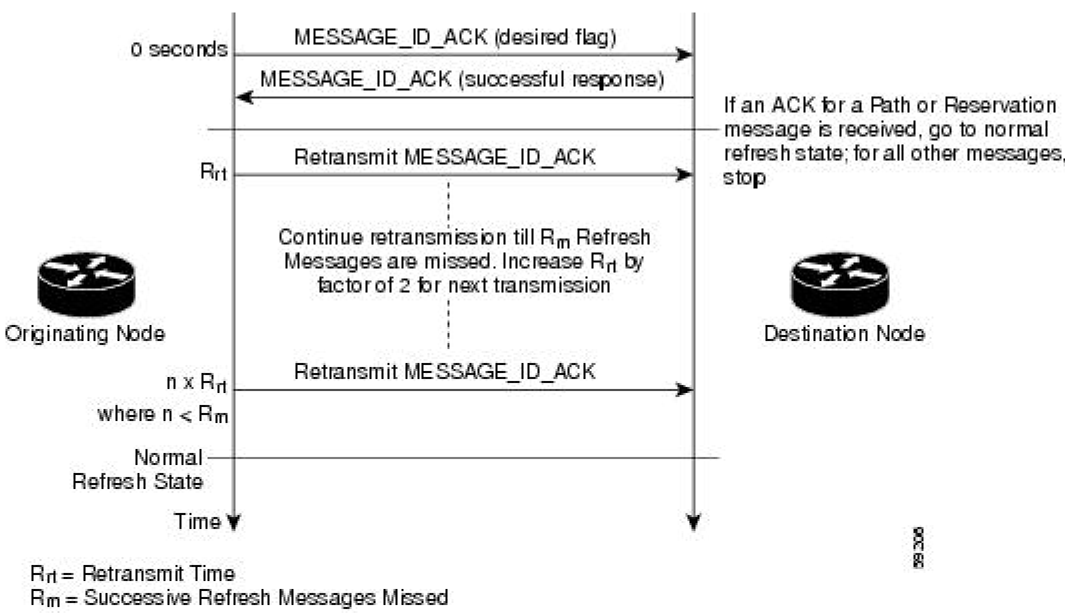
**Note** RSVP packets consist of headers that identify the types of messages, and object fields that contain attributes and properties describing how to interpret and act on the content.

# Types of Messages in RSVP Refresh Reduction and Reliable Messaging

The RSVP Refresh Reduction and Reliable Messaging feature (see the figure below) includes refresh reduction, which improves the scalability, latency, and reliability of RSVP signaling by introducing the following extensions:

- Reliable messages (MESSAGE_ID, MESSAGE_ID_ACK objects, and ACK messages)
- Bundle messages (reception and processing only)
- Summary refresh messages (MESSAGE_ID_LIST and MESSAGE_ID_NACK objects)

*Figure 5* ***RSVP Refresh Reduction and Reliable Messaging***




- Reliable Messages, page 150
- Bundle Messages, page 150
- Summary Refresh Messages, page 150

## Reliable Messages

The reliable messages extension supports dependable message delivery among neighboring routers by implementing an acknowledgment mechanism that consists of a MESSAGE_ID object and a MESSAGE_ID_ACK object. The acknowledgments can be transmitted in an ACK message or piggybacked in other RSVP messages.

Each RSVP message contains one MESSAGE_ID object. If the ACK_Desired flag field is set within the MESSAGE_ID object, the receiver transmits a MESSAGE_ID_ACK object to the sender to confirm delivery.

## Bundle Messages

A bundle message consists of several standard RSVP messages that are grouped into a single RSVP message.

A bundle message must contain at least one submessage. A submessage can be any RSVP message type other than another bundle message. Submessage types include Path, PathErr, Resv, ResvTear, ResvErr, ResvConf, and ACK.

Bundle messages are addressed directly to the RSVP neighbor. The bundle header immediately follows the IP header, and there is no intermediate transport header.

When a router receives a bundle message that is not addressed to one of its local IP addresses, it forwards the message.

**Note** Bundle messages can be received, but not sent.

## Summary Refresh Messages

A summary refresh message supports the refreshing of RSVP state without the transmission of conventional Path and Resv messages. Therefore, the amount of information that must be transmitted and processed to maintain RSVP state synchronization is greatly reduced.

A summary refresh message carries a set of MESSAGE_ID objects that identify the Path and Resv states that should be refreshed. When an RSVP node receives a summary refresh message, the node matches each received MESSAGE_ID object with the locally installed Path or Resv state. If the MESSAGE_ID objects match the local state, the state is updated as if a standard RSVP refresh message were received. However, if a MESSAGE_ID object does not match the receiver’s local state, the receiver notifies the sender of the summary refresh message by transmitting a MESSAGE_ID_NACK object.

When a summary refresh message is used to refresh the state of an RSVP session, the transmission of conventional refresh messages is suppressed. The summary refresh extension cannot be used for a Path or Resv message that contains changes to a previously advertised state. Also, only a state that was previously advertised in Path or Resv messages containing MESSAGE_ID objects can be refreshed by using a summary refresh message.

## Benefits of RSVP Refresh Reduction and Reliable Messaging

#### Enhanced Network Performance

Refresh reduction reduces the volume of steady-state network traffic generated, the amount of CPU resources used, and the response time, thereby enhancing network performance.

#### Improved Message Delivery

The MESSAGE_ID and the MESSAGE_ID_ACK objects ensure the reliable delivery of messages and support rapid state refresh when a network problem occurs. For example, MESSAGE_ID_ACK objects are used to detect link transmission losses.

# How to Configure RSVP Refresh Reduction and Reliable Messaging



## Enabling RSVP on an Interface

Perform the following task to enable RSVP on an interface.

#### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp bandwidth** [*interface-kbps* [*sub-pool*]]
5. **end**

#### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br><br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br><br>**Example:**<br><br>`Router(config)# interface Ethernet1` | Enters interface configuration mode.<br><br>• The *type*and *number* arguments identify the interface to be configured. |
| **Step 4** | **ip rsvp bandwidth** [*interface-kbps* [*sub-pool*]]<br><br>**Example:**<br><br>`Router(config-if)# ip rsvp bandwidth 7500 7500` | Enables RSVP on an interface.<br><br>• The optional *interface-kbps* and *sub-pool*arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10000000, and from 0 to 10000000, respectively. |
| **Step 5** | **end**<br><br>**Example:**<br><br>`Router(config-if)# end` | Returns to privileged EXEC mode. |

# Enabling RSVP Refresh Reduction

Perform the following task to enable RSVP refresh reduction.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling refresh reduction**
4. **end**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br><br>`Router> enable` | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br><br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **ip rsvp signalling refresh reduction**<br><br>**Example:**<br>`Router(config)# ip rsvp signalling refresh reduction` | Enables refresh reduction. |
| **Step 4** | **end**<br><br>**Example:**<br>`Router(config)#` **end** | Returns to privileged EXEC mode. |

# Verifying RSVP Refresh Reduction and Reliable Messaging

Perform the following task to verify that the RSVP Refresh Reduction and Reliable Messaging feature is functioning.

### SUMMARY STEPS

1. **enable**
2. **clear ip rsvp counters** [**confirm**]
3. **show ip rsvp**
4. **show ip rsvp counters [ interface** *interface-unit* **| summary | neighbor ]**
5. **show ip rsvp interface [** *interface-type interface-number* **] [ detail ]**
6. **show ip rsvp neighbor [ detail ]**

### DETAILED STEPS

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br><br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **clear ip rsvp counters** [**confirm**]<br><br>**Example:**<br><br>`Router# clear ip rsvp counters` | (Optional) Clears (sets to zero) all IP RSVP counters that are being maintained by the router. |
| **Step 3** | **show ip rsvp**<br><br>**Example:**<br><br>`Router# show ip rsvp` | (Optional) Displays RSVP rate-limiting, refresh-reduction, and neighbor information. |
| **Step 4** | **show ip rsvp counters [ interface** *interface-unit* \| **summary** \| **neighbor ]**<br><br>**Example:**<br><br>`Router# show` **ip rsvp counters summary** | (Optional) Displays the number of RSVP messages that were sent and received on each interface.<br><br>• The optional **summary** keyword displays the cumulative number of RSVP messages sent and received by the router over all interfaces. |
| **Step 5** | **show ip rsvp interface [** *interface-type interface-number* **] [ detail ]**<br><br>**Example:**<br><br>`Router# show ip rsvp interface detail` | (Optional) Displays information about interfaces on which RSVP is enabled including the current allocation budget and maximum available bandwidth.<br><br>• The optional **detail** keyword displays the bandwidth and signaling parameters. |
| **Step 6** | **show ip rsvp neighbor [ detail ]**<br><br>**Example:**<br><br>`Router# show ip rsvp neighbor detail` | (Optional) Displays RSVP-neighbor information including IP addresses.<br><br>• The optional **detail** keyword displays the current RSVP neighbors and identifies if the neighbor is using IP, User Datagram Protocol (UDP), or RSVP encapsulation for a specified interface or all interfaces. |

# Configuration Examples for RSVP Refresh Reduction and Reliable Messaging



## Example RSVP Refresh Reduction and Reliable Messaging

In the following example, RSVP refresh reduction is enabled:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# interface Ethernet1
Router(config-if)# ip rsvp bandwidth 7500 7500
Router(config-if)# exit
Router(config)# ip rsvp signalling refresh reduction
Router(config)# end
```

The following example verifies that RSVP refresh reduction is enabled:

```
Router# show running-config
Building configuration...
Current configuration : 1503 bytes
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname Router
!
no logging buffered
logging rate-limit console 10 except errors
!
ip subnet-zero
ip cef
!
ip multicast-routing
no ip dhcp-client network-discovery
lcp max-session-starts 0
mpls traffic-eng tunnels
!
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
 ip rsvp bandwidth 1705033 1705033
!
interface Tunnel777
 no ip address
 shutdown
!
interface Ethernet0
 ip address 192.168.0.195 255.0.0.0
 no ip mroute-cache
 media-type 10BaseT
!
interface Ethernet1
 ip address 192.168.5.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 no ip mroute-cache
 media-type 10BaseT
 ip rsvp bandwidth 7500 7500
!
interface Ethernet2
 ip address 192.168.1.2 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip pim dense-mode
 no ip mroute-cache
 media-type 10BaseT
 mpls traffic-eng tunnels
 ip rsvp bandwidth 7500 7500
!
interface Ethernet3
 ip address 192.168.2.2 255.255.255.0
 ip pim dense-mode
 media-type 10BaseT
 mpls traffic-eng tunnels
!
!
router eigrp 17
```

```
 network 192.168.0.0
 network 192.168.5.0
 network 192.168.12.0
 network 192.168.30.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip classless
no ip http server
ip rsvp signalling refresh reduction
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
 transport input pad v120 telnet rlogin udptn
!
end
```

# Additional References

The following sections provide references related to the RSVP Refresh Reduction and Reliable Messaging feature.

### Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples | *Cisco IOS Quality of Service Solutions Command Reference* |
| QoS features including signaling, classification, and congestion management | "Quality of Service Overview" module |

### Standards

| Standard | Title |
|---|---|
| None | -- |

### 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 |
|---|---|
| RFC 2205 | *Resource Reservation Protocol* |
| RFC 2206 | *RSVP Management Information Base Using SMIv2* |
| RFC 2209 | *RSVP--Version 1 Message Processing Rules* |
| RFC 2210 | *The Use of RSVP with IETF Integrated Services* |
| RFC 2211/2212 | *Specification of the Controlled-Load Network Element Service* |
| RFC 2702 | *Requirements for Traffic Engineering over MPLS* |
| RFC 2749 | *Common Open Policy Service (COPS) Usage for RSVP* |
| RFC 2750 | *RSVP Extensions for Policy Control* |
| RFC 2814 | *SBM Subnet Bandwidth Manager: A Protocol for RSVP-based Admission Control over IEEE 802-style Networks* |
| RFC 2961 | *RSVP Refresh Overhead Reduction Extensions* |
| RFC 2996 | *Format of the RSVP DCLASS Object* |

### 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 |