MPLS Traffic Engineering and Enhancements

This feature module describes MPLS traffic engineering and enhancements for Release 12.1(3)T. The document includes the following sections:

Feature Overview

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

- 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.

Why Use 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 the 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 IOS 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 head-end 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.

For more information about MPLS (previously referred to as Tag Switching), see the following Cisco documentation:

- *Cisco IOS Switching Services Configuration Guide*, "Multiprotocol Label Switching" chapter
- *Cisco IOS Switching Services Command Reference*, "Switching Commands Introduction" chapter

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 head-end 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 head-end 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.

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 head-end router. For each of those TE tunnels, the router at the tail-end 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 tail-end 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

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 Figure 1.

Figure 1   Sample Topology of Parallel Native Paths and Paths Over TE Tunnels
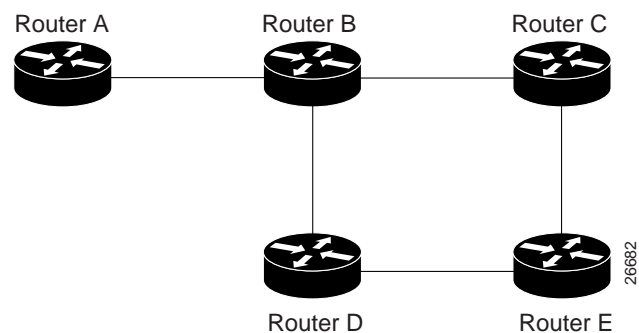
If parallel native IP paths and paths over TE tunnels are available, the following implementations allow you to force traffic to flow over TE tunnels only or only over native IP paths. Assume that all links have the same cost and that a TE tunnel is set up from Router A to Router D.

- 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 tail-end 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 tail-end 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 tail-end router, but also for each route downstream of this tail-end 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 Figure 2.

Figure 2 *Topology That Has No Traffic Engineering Tunnel*
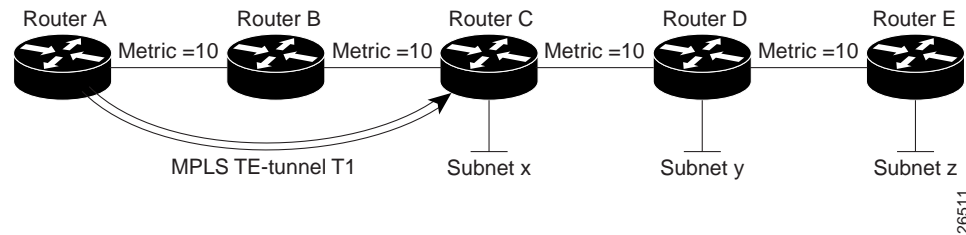
If there is no TE tunnel, Router A installs routes x, y, and z and assigns metrics 20, 30, and 40 respectively. Suppose that Router A has a TE tunnel T1 to Router C. If the relative metric –5 is used on tunnel T1, the routers x, y, and z have the installed metrics of 15, 25, and 35. If an absolute metric 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.

Transitioning an IS-IS Network to a New Technology

A new flavor of IS-IS 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 this new flavor of IS-IS.

Note Running MPLS traffic engineering over an existing IS-IS network requires a transition to a new flavor of IS-IS. However, running MPLS traffic engineering over OSPF does **not** require any similar network transition.

New Extensions for the IS-IS Routing Protocol

New 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.

The Problem in Theory

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 Problem in Practice

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 "TLV Configuration Commands."

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 has a new router isis command line interface (CLI) subcommand called metric-style. Once you are in the router IS-IS subcommand 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

For more information about the commands, see the "Command Reference" section in this document.

You can use either of two transition schemes when you are using the metric-style commands:

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

Implementation in IOS

IOS implements both transition solutions. Network administrators can choose the solution that suits them best. For test networks, the first solution is ideal (go to "First Solution for Transitioning an IS-IS Network to a New Technology"). For a real transition, both solutions can be used. The first solution requires fewer steps and less configuration. Only the largest networks that do not want to risk doubling their LSPDB during transition need to use the second solution (go to "Second Solution for Transitioning an IS-IS Network to a New Technology").

Benefits

MPLS traffic engineering has the following benefits:

- Higher return on network backbone infrastructure investment. The best route between a pair of POPs is determined, taking into account the constraints of the backbone network and the total traffic load on the backbone.
- Reduction in operating costs. Costs are reduced because numerous important processes are automated, including setup, configuration, mapping, and selection of MPLS traffic engineered (MPLS TE) tunnels across a Cisco 12000 series backbone.

Restrictions

The following restrictions apply to MPLS traffic engineering:

- MPLS traffic engineering currently supports only a single IS-IS level or OSPF area.

- Currently, 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.

Related Features and Technologies

The MPLS traffic engineering feature is related to the IS-IS, OSPF, RSVP, and MPLS features (formerly referred to as Tag Switching). These features are presented in Cisco product documentation (see the sections on "Related Documents" and "How MPLS Traffic Engineering Works").

Related Documents

- *Cisco IOS IP and IP Routing Configuration Guide*, "Configuring Integrated IS-IS" chapter
- *Cisco IOS IP and IP Routing Command Reference,* "Integrated IS-IS Commands" chapter
- Cisco *IOS IP and IP Routing Configuration Guide*, "Configuring OSPF" chapter
- *Cisco IOS IP and IP Routing Command Reference*, "OSPF Commands" chapter
- *Cisco IOS Quality of Service Solutions Command Reference*, "RSVP Commands" chapter
- *Cisco IOS Switching Services Configuration Guide*, "Multiprotocol Label Switching" chapter
- *Cisco IOS Switching Services Command Reference*, "Switching Commands Introduction" chapter

Supported Platforms

- Cisco 7200 Series
- Cisco 7500 Series
- Cisco 12000 Series

Supported Standards, MIBs, and RFCs

Standards

None.

MIBs

There are no MIBs supported by this feature.

RFCs

- RFC 2205, Resource ReSerVation Protocol (RSVP)

- RFC 1142, IS-IS
- RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments
- RFC 2328, OSPF Version 2
- RFC 2370, The OSPF Opaque LSA Option

Prerequisites

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

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

Configuration Tasks

Perform the following tasks before you enable MPLS traffic engineering:

- Turn on MPLS tunnels
- Turn on Cisco Express Forwarding (CEF)
- Turn on IS-IS or OSPF

Perform the following tasks to configure MPLS traffic engineering:

- Configuring a Device to Support Tunnels
- Configuring an Interface to Support RSVP-Based Tunnel Signaling and IGP Flooding
- Configuring IS-IS for MPLS Traffic Engineering
- Configuring OSPF for MPLS Traffic Engineering
- Configuring an MPLS Traffic Engineering Tunnel
- Configuring an MPLS Traffic Engineering Tunnel that an IGP Can Use

Configuring a Device to Support Tunnels

To configure a device to support tunnels, perform the following steps in configuration mode.

	Command	Purpose
Step 1	Router(config)# **ip cef**	Enables standard CEF operation.
		For information about CEF configuration and the command syntax, see the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference*.
Step 2	Router(config)# **mpls traffic-eng tunnels**	Enables the MPLS traffic engineering tunnel feature on a device.

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

To configure an interface to support RSVP-based tunnel signaling and IGP flooding, perform these steps in interface configuration mode:

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

	Command	Purpose
Step 1	Router(config-if)# **mpls traffic-eng tunnels**	Enables MPLS traffic engineering tunnels on an interface.
Step 2	Router(config-if)# **ip rsvp bandwidth** *bandwidth*	Enables RSVP for IP on an interface and specifies the amount of bandwidth that will be reserved. For a description of the ip rsvp command syntax, see the *Cisco IOS Quality of Service Solutions Command Reference*.

Configuring IS-IS for MPLS Traffic Engineering

To configure IS-IS for MPLS traffic engineering, perform the steps described below. For a description of the IS-IS commands (excluding the IS-IS traffic engineering commands), see the *Cisco IOS IP and IP Routing Command Reference*.

	Command	Purpose
Step 1	Router(config)# **router isis**	Enables IS-IS routing and specifies an IS-IS process for IP. This command places you in router 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 router-id loopback0**	Specifies that the traffic engineering router identifier for the node is the IP address associated with interface loopback0.
Step 4	Router(config-router)# **metric-style wide**	Configures a router to generate and accept only new-style TLVs.

Configuring OSPF for MPLS Traffic Engineering

To configure OSPF for MPLS traffic engineering, perform the steps described below. For a description of the OSPF commands (excluding the OSPF traffic engineering commands), see the *Cisco IOS IP and IP Routing Command Reference*.

	Command	Purpose
Step 1	Router(config)# **router ospf** *process-id*	Configures an OSPF routing process for IP. You are placed in router configuration mode. 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 2	Router(config-router)# **mpls traffic-eng area 0**	Turns on MPLS traffic engineering for OSPF area 0.
Step 3	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.

Configuring an MPLS Traffic Engineering Tunnel

To configure an MPLS traffic engineering tunnel, perform these steps in interface configuration mode. This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

	Command	Purpose
Step 1	Router(config)# **interface tunnel**	Configures an interface type and enters interface configuration mode.
Step 2	Router(config)# **ip unnumbered loopback0**	Gives the tunnel interface an IP address. An MPLS traffic engineering tunnel interface should be unnumbered because it represents a unidirectional link.
Step 3	Router(config-if)# **tunnel destination** *A.B.C.D*	Specifies the destination for a tunnel.
Step 4	Router(config-if)# **tunnel mode mpls traffic-eng**	Sets the tunnel encapsulation mode to MPLS traffic engineering.
Step 5	Router(config-if)# **tunnel mpls traffic-eng bandwidth** *bandwidth*	Configures the bandwidth for the MPLS traffic engineering tunnel.
Step 6	Router(config-if)# **tunnel mpls traffic-eng path-option** *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number*}} [**lockdown**]	Configures the tunnel to use a named IP explicit path or a path dynamically calculated from the traffic engineering topology database. A dynamic path is used if an explicit path is currently unavailable.

Configuring an MPLS Traffic Engineering Tunnel that an IGP Can Use

To configure an MPLS traffic engineering tunnel that an IGP can use, perform these steps in interface configuration mode. This tunnel has two path setup options: a preferred explicit path and a backup dynamic path.

|	Command	Purpose
Step 1	`Router(config-if)# interface tunnel1`	Configures an interface type and enters interface configuration mode.
Step 2	`Router(config-if)# tunnel mpls traffic-eng autoroute announce`	Causes the IGP to use the tunnel in its enhanced SPF calculation.

Configuration Examples

This section provides the following configuration examples:

- Configuring MPLS Traffic Engineering Using IS-IS
- Configuring MPLS Traffic Engineering Using OSPF
- Configuring an MPLS Traffic Engineering Tunnel
- Configuring Enhanced SPF Routing Over a Tunnel

Figure 3 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
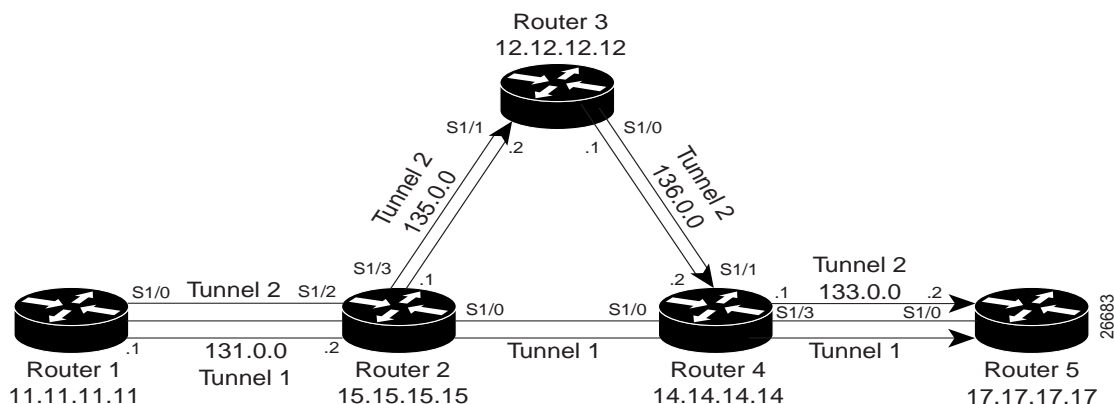
Configuring MPLS Traffic Engineering Using IS-IS

This example lists the commands you enter to configure MPLS traffic engineering with IS-IS routing enabled
(see Figure 3).

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

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 11.11.11.11 255.255.255.255
ip router isis

interface s1/0
ip address 131.0.0.1 255.255.0.0
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
```

Configuring MPLS Traffic Engineering Using OSPF

This example lists the commands you enter to configure MPLS traffic engineering with OSPF routing enabled (see Figure 3).

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

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 11.11.11.11 255.255.255.255

interface s1/0
ip address 131.0.0.1 255.255.0.0
mpls traffic-eng tunnels
  ip rsvp bandwidth 1000
```

Router 1—OSPF Configuration

To enable OSPF, enter the following commands:

```
router ospf 0
network 131.0.0.0.0.0.255.255 area 0
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
```

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

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

```
interface tunnel1
  ip unnumbered loopback 0
  tunnel destination 17.17.17.17
  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 131.0.0.1
 next-address 135.0.0.1
 next-address 136.0.0.1
 next-address 133.0.0.1
```

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 17.17.17.17
  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
```

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

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 17.17.17.17
show mpls traffic-eng autoroute
ping 17.17.17.17
show interface tunnel1 accounting
show interface s1/0 accounting
```

Command Reference

This section documents new or modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **append-after**
- **index**
- **ip explicit-path**
- **list**
- **metric-style narrow**
- **metric-style transition**
- **metric-style wide**
- **mpls traffic-eng**
- **mpls traffic-eng administrative-weight**
- **mpls traffic-eng area**
- **mpls traffic-eng attribute-flags**
- **mpls traffic-eng flooding thresholds**
- **mpls traffic-eng link-management timers bandwidth-hold**
- **mpls traffic-eng link-management timers periodic-flooding**
- **mpls traffic-eng logging lsp**
- **mpls traffic-eng logging tunnel**
- **mpls traffic-eng reoptimize**
- **mpls traffic-eng reoptimize events**
- **mpls traffic-eng reoptimize timers frequency**
- **mpls traffic-eng router-id**
- **mpls traffic-eng signaling advertise implicit-null**
- **mpls traffic-eng tunnels (configuration)**
- **mpls traffic-eng tunnels (interface)**
- **next-address**
- **show ip explicit-paths**
- **show ip ospf database opaque-area**
- **show ip ospf mpls traffic-eng**
- **show ip rsvp host**
- **show isis database verbose**
- **show isis mpls traffic-eng adjacency-log**
- **show isis mpls traffic-eng advertisements**
- **show isis mpls traffic-eng tunnel**
- **show mpls traffic-eng autoroute**
- **show mpls traffic-eng link-management admission-control**

- **show mpls traffic-eng link-management advertisements**
- **show mpls traffic-eng link-management bandwidth-allocation**
- **show mpls traffic-eng link-management igp-neighbors**
- **show mpls traffic-eng link-management interfaces**
- **show mpls traffic-eng link-management summary**
- **show mpls traffic-eng topology**
- **show mpls traffic-eng topology path**
- **show mpls traffic-eng tunnels**
- **show mpls traffic-eng tunnels summary**
- **tunnel mode mpls traffic-eng**
- **tunnel mpls traffic-eng affinity**
- **tunnel mpls traffic-eng autoroute announce**
- **tunnel mpls traffic-eng autoroute metric**
- **tunnel mpls traffic-eng bandwidth**
- **tunnel mpls traffic-eng path-option**
- **tunnel mpls traffic-eng priority**

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the "pipe" character (|)**,** one of the keywords **begin**, **include**, or **exclude,** and an expression that you want to search or filter on:

command **|** {**begin** | **include** | **exclude**} *regular-expression*

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression "PeakRate" appears:

show atm vc / begin PeakRate

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

append-after

To insert a path entry after a specified index number, use the **append-after** IP explicit path subcommand.

> **append-after** *index command*

Syntax Description		
index		Previous index number. Valid values are from 0 to 65534.
command		An IP explicit path configuration command that creates a path entry. (For this release you can use only the **next-address** command, which specifies the next IP address in the explicit path.)

Defaults

No default behavior or values.

Command Modes

IP explicit path subcommand

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, th**e next-address** subcommand is inserted after index 5:

```
Router(config-ip-expl-path)# append-after 5 next-address 3.3.27.3
```

Related Commands

Command	Description
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit path(s).
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

index

To insert or modify a path entry at a specific index, use the **index** ip explicit path subcommand. Use the **no** form of this command to disable this feature.

> **index** *index command*

> **no index** *index*

Syntax Description

index	Index number at which the path entry will be inserted or modified. Valid values are from 0 to 65534.
command	An IP explicit path configuration command that creates or modifies a path entry. (Currently you can use only the **next-address** command.)

Defaults

No default behavior or values.

Command Modes

IP explicit path subcommand

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the **next-address** command is inserted at index 6:

```
Router(cfg-ip-expl-path)# index 6 next-address 3.3.29.3

Explicit Path identifier 6:
    6: next-address 3.3.29.3
```

Related Commands

Command	Description
append-after	Similar to the **index** subcommand, except that this command inserts the new path entry after the specified index number. Commands might be renumbered as a result.
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
list	Displays all or part of the explicit path(s).
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

ip explicit-path

To enter the subcommand mode for Internet Protocol (IP) explicit paths and create or modify the specified path, use the **ip explicit-path** configuration command. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path. Use the **no** form of this command to disable this feature.

> **ip explicit-path** { **name** *word* | **identifier** *number* } [{**enable** | **disable** }]

> **no explicit-path** { **name** *word* | **identifier** *number* }

Syntax Description		
name *word*	Name of the explicit path.
identifier *number*	Number of the explicit path. Valid values are from 1 to 65535.
enable	Enables the path.
disable	Prevents the path from being used for routing while it is being configured.

Command Modes   Configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.

Examples

In the following example, the explicit path subcommand mode for IP explicit paths is entered and a path with the number 500 is created:

```
Router(config)# ip explicit-path identifier 500

Router(config-ip-expl-path)#
```

Related Commands	Command	Description
	append-after	Similar to the **index** subcommand, except that this command inserts the new path entry after the specified index number. Commands might be renumbered as a result.
	index	Inserts or modifies a path entry at a specific index.
	list	Displays all or part of the explicit path(s).
	next-address	Specifies the next IP address in the explicit path.
	show ip explicit-paths	Displays the configured IP explicit paths.

list

To show all or part of the explicit path or paths, use the **list** ip explicit path subcommand.

list [{ *starting index number* }]

Syntax Description

starting index number	Index number at which the explicit path(s) will start to be displayed. Valid values are from 1 to 65535.

Defaults

No default behavior or values.

Command Modes

IP explicit path subcommand

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following example shows the explicit path starting at index number 2:

```
Router(cfg-ip-expl-path)# list

Explicit Path name Joe:
    1:next-address 10.0.0.1
    2:next-address 10.0.0.2

Router(cfg-ip-expl-path)# list 2

Explicit Path name Joe:
    2:next-address 10.0.0.2
Router(cfg-ip-expl-path)#
```

Related Commands

Command	Description
append-after	Similar to the **index** subcommand, except that this command inserts the new path entry after the specified index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the subcommand mode for IP explicit paths, and creates or modifies the specified path.
next-address	Specifies the next IP address in the explicit path.
show ip explicit-paths	Displays the configured IP explicit paths.

metric-style narrow

To configure a router running IS-IS so that it generates and accepts old-style type, length, and value objects (TLVs), use the **metric-style narrow** router configuration command. Use the **no** form of this command to disable this feature.

metric-style narrow [**transition**] [{ **level-1** | **level-2** | **level-1-2** }]

no metric-style narrow [**transition**] [{ **level-1** | **level-2** | **level-1-2** }]

Syntax Description

transition	(Optional) Instructs the router to use both old- and new-style TLVs.
level-1	Enables this command on routing level 1.
level-2	Enables this command on routing level 2.
level-1-2	Enables this command on routing levels 1 and 2.

Defaults

The MPLS traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the router is instructed to generate and accept old-style TLVs on router level 1:

```
Router(config-router)# metric-style narrow level-1
```

Related Commands

Command	Description
metric-style transition	Configures a router to generate both old-style and new-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style transition

To configure a router running IS-IS so that it generates and accepts both old-style and new-style type, length, and value objects (TLVs), use the **metric-style transition** router configuration command. Use the **no** form of this command to disable this feature.

metric-style transition [{ **level-1** | **level-2** | **level-1-2** }]

no metric-style transition [{ **level-1** | **level-2** | **level-1-2** }]

Syntax Description

level-1	Enables this command on routing level 1.
level-2	Enables this command on routing level 2.
level-1-2	Enables this command on routing levels 1 and 2.

Defaults

The MPLS traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, a router is configured to generate and accept both old-style and new-style TLVs on router level 2:

```
Router(config-router)# metric-style transition level-2
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style wide	Configures a router to generate and accept only new-style TLVs.

metric-style wide

To configure a router running IS-IS so that it generates and accepts only new-style type, length, and value objects (TLVs), use the **metric-style wide** router configuration command. Use the **no** form of this command to disable this feature.

metric-style wide [**transition**] [{ **level-1** | **level-2** | **level-1-2** }]

no metric-style wide [**transition**] [{ **level-1** | **level-2** | **level-1-2** }]

Syntax Description

transition	(Optional) Instructs the router to accept both old- and new-style TLVs.
level-1	Enables this command on routing level 1.
level-2	Enables this command on routing level 2.
level-1-2	Enables this command on routing levels 1 and 2.

Defaults

The MPLS traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

Command Modes

Router configuration

Command History

Release	Modification
Release 12.0(5)S	This command was introduced.

Usage Guidelines

If you enter the **metric-style wide** command, a router generates and accepts only new-style TLVs. Therefore, the router uses less memory and other resources than it would if it generated both old-style and new-style TLVs.

This style is appropriate for enabling MPLS traffic engineering across an entire network.

> **Note** This discussion of metric styles and transition strategies is oriented towards traffic engineering deployment. Other commands and models could be appropriate if the new-style TLVs are desired for other reasons. For example, a network might require wider metrics, but might not use traffic engineering.

Examples

In the following example, a router is configured to generate and accept only new-style TLVs on level 1:

```
Router(config-router)# metric-style wide level-1
```

Related Commands

Command	Description
metric-style narrow	Configures a router to generate and accept old-style TLVs.
metric-style transition	Configures a router to generate and accept both old-style and new-style TLVs.

mpls traffic-eng

To configure a router running IS-IS so that is floods MPLS traffic engineering link information into the indicated IS-IS level, use the **mpls traffic-eng** router configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng { **level-1** | **level-2** }

no mpls traffic-eng { **level-1** | **level-2** }

Syntax Description		
	level-1	Floods MPLS traffic engineering link information into IS-IS level 1.
	level-2	Floods MPLS traffic engineering link information into IS-IS level 2.

Defaults

Flooding is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This command, which is part of the routing protocol tree, causes link resource information (such as available bandwidth) for appropriately configured links to be flooded in the IS-IS link state database.

Examples

In the following example, MPLS traffic engineering is turned on for IS-IS level 1:

```
Router(config-router)# mpls traffic-eng level-1
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.

mpls traffic-eng administrative-weight

To override the Interior Gateway Protocol (IGP) administrative weight (cost) of the link, use the **mpls traffic-eng administrative-weight** interface configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng administrative-weight *weight*

no mpls traffic-eng administrative-weight

Syntax Description

weight	Cost of the link.

Defaults

IGP cost of the link.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, the IGP cost of the link is overridden, and the cost is set to 20:

```
Router(config-if)# mpls traffic-eng administrative-weight 20
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the user-specified attribute flags for an interface.

mpls traffic-eng area

To configure a router running Open Shortest Path First (OSPF) MPLS so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** router configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng area *num*

no mpls traffic-eng area *num*

Syntax Description

num	The OSPF area on which MPLS traffic engineering is enabled.

Defaults

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This command is in the routing protocol configuration tree and is supported for both OSPF and IS-IS. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single level can be enabled for traffic engineering.

Examples

In the following example, a router running OSPF MPLS is configured to flood traffic engineering for OSPF 0:

```
Router(config-router)# mpls traffic-eng area 0
```

Related Commands

Command	Description
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
network area	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.
router ospf	Configures an OSPF routing process on a router.

mpls traffic-eng attribute-flags

To set the user-specified attribute flags for the interface, use the **mpls traffic-eng attribute-flags** interface configuration command. The interface is flooded globally so that it can be used as a tunnel head-end path selection criterion. Use the **no** form of this command to disable this feature.

mpls traffic-eng attribute-flags *attributes*

no mpls traffic-eng attribute-flags

Syntax Description

attributes	Links attributes that will be compared to a tunnel's affinity bits during selection of a path.
	Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits) where the value of an attribute is 0 or 1.

Defaults

0x0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This command assigns attributes to a link so that tunnels with matching attributes (represented by their affinity bits) prefer this link instead of others that do not match.

Examples

In the following example, the attribute flags are set to 0x0101:

```
Router(config-if)# mpls traffic-eng attribute-flags 0x0101
```

Related Commands

Command	Description
mpls traffic-eng administrative-weight	Overrides the Interior Gateway Protocol (IGP) administrative weight of the link.
tunnel mpls traffic-eng affinity	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.

mpls traffic-eng flooding thresholds

To set a link's reserved bandwidth thresholds, use the **mpls traffic-eng flooding thresholds** interface configuration command. Use the **no** form of this command to return to the default settings.

mpls traffic-eng flooding thresholds { **down** | **up** } *percent* [*percent* ...]

no mpls traffic-eng flooding thresholds { **down** | **up** }

Syntax Description		
down	Sets the thresholds for decreased resource availability.	
up	Sets the thresholds for increased resource availability.	
percent [*percent*]	Bandwidth threshold level. For **down**, valid values are from 0 through 99. For **up**, valid values are from 1 through 100.	

The default for **down** is 100, 99, 98, 97, 96, 95, 90, 85, 80, 75, 60, 45, 30, 15.

The default for **up** is 15, 30, 45, 60, 75, 80, 85, 90, 95, 97, 98, 99, 100.

Command Modes   Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines   When a threshold is crossed, MPLS traffic engineering link management advertises updated link information. If no thresholds are crossed, changes can be flooded periodically unless periodic flooding was disabled.

Examples   In the following example, the link's reserved bandwidth is set for decreased resource availability (down) and for increased resource availability (up) thresholds:

```
Router(config-if)# mpls traffic-eng flooding thresholds down 100 75 25
Router(config-if)# mpls traffic-eng flooding thresholds up 25 50 100
```

Related Commands

Command	Description
mpls traffic-eng link-management timers periodic-flooding	Sets the length of the interval used for periodic flooding.
show mpls traffic-eng link-management advertisements	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.

mpls traffic-eng link-management timers bandwidth-hold

To set the length of time that bandwidth is held for an RSVP Path (setup) message while you wait for the corresponding RSVP Resv message to come back, use the **mpls traffic-eng link-management timers bandwidth-hold** configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng link-management timers bandwidth-hold *hold-time*

no mpls traffic-eng link-management timers bandwidth-hold

Syntax Description	*hold-time* Length of time that bandwidth can be held. Valid values are from 1 to 300 seconds.

Defaults 15 seconds.

Command Modes Configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

In the following example, bandwidth is set to be held for 10 seconds:

```
Router(config)# mpls traffic-eng link-management timers bandwidth-hold 10
```

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.

mpls traffic-eng link-management timers periodic-flooding

To set the length of the interval for periodic flooding, use the **mpls traffic-eng link-management timers periodic-flooding** configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng link-management timers periodic-flooding *interval*

no mpls traffic-eng link-management timers periodic-flooding

Syntax Description

interval	Length of the interval, in seconds, for periodic flooding. Valid values are from 0 to 3600. A value of 0 turns off periodic flooding. If you set this value from 1 to 29, it is treated as 30.

Defaults

180 seconds (3 minutes).

Command Modes

Configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

Use this command to advertise link state information changes that do not trigger immediate action. Example: a change to the amount of allocated bandwidth that does not cross a threshold.

Examples

In the following example, the interval length for periodic flooding is set to 120 seconds:

```
Router(config)# mpls traffic-eng link-management timers periodic-flooding 120
```

Related Commands

Command	Description
mpls traffic-eng flooding thresholds	Sets a link's reserved bandwidth thresholds.

mpls traffic-eng logging lsp

To log certain traffic engineering label-switched path (LSP) events, use the **mpls traffic-eng logging lsp** router configuration command. Use the **no** form of this command to disable this feature.

> **mpls traffic-eng logging lsp** { **path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns** } [*aclnum*]

> **no mpls traffic-eng logging lsp** { **path-errors** | **reservation-errors** | **preemption** | **setups** | **teardowns** } [*aclnum*]

Syntax Description

path-errors	Logs RSVP path errors for traffic engineering LSPs.
reservation-errors	Logs RSVP reservation errors for traffic engineering LSPs.
preemption	Logs events related to the preemption of traffic engineering LSPs.
setups	Logs events related to the establishment of traffic engineering LSPs.
teardowns	Logs events related to the removal of traffic engineering LSPs.
aclnum	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for LSPs that match the access list.

Defaults

Logging of LSP events is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, path errors are logged for LSPs that match access list 3:

```
Router(config)# mpls traffic-eng logging lsp path-errors 3
```

Related Commands

Command	Description
access-list (extended)	Defines an extended IP access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging tunnel	Logs certain traffic engineering tunnel events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng logging tunnel

To log certain traffic engineering tunnel events, use the **mpls traffic-eng logging tunnel** router configuration command. Use the **no** form of this command to disable this feature.

> **mpls traffic-eng logging tunnel lsp-selection** [*aclnum*]

> **no mpls traffic-eng logging tunnel lsp-selection** [*aclnum*]

Syntax Description

lsp-selection	Logs events related to the selection of an LSP for a traffic engineering tunnel.
aclnum	(Optional) Uses the specified access list to filter the events that are logged. Logs events only for tunnels that match the access list.

Defaults

Logging of tunnel events is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, traffic engineering tunnel events associated with access list 3 are logged:

```
Router(config)# mpls traffic-eng logging tunnel lsp-selection 3
```

Related Commands

Command	Description
access-list (extended)	Creates an extended access list.
logging console	Limits the number of messages logged to the console.
mpls traffic-eng logging lsp	Logs certain traffic engineering LSP events.
show logging	Displays the messages that are logged in the buffer.

mpls traffic-eng reoptimize

To force immediate reoptimization of all traffic engineering tunnels, use the **mpls traffic-eng reoptimize** EXEC command.

mpls traffic-eng reoptimize

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples   In the following example, all traffic engineering tunnels are immediately reoptimized:

```
Router2# mpls traffic-eng reoptimize
```

mpls traffic-eng reoptimize events

To turn on automatic reoptimization of MPLS traffic engineering when certain events occur, such as when an interface becomes operational, use the **mpls traffic-eng reoptimize events** router configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng reoptimize events {**link-up**}

no mpls traffic-eng reoptimize events {**link-up**}

Syntax Description

link-up	Triggers automatic reoptimization whenever an interface becomes operational.

Defaults

Event-based reoptimization is disabled.

Command Modes

Router configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, automatic reoptimization is turned on whenever an interface becomes operational:

```
Router(config)# mpls traffic-eng reoptimize events link-up
```

Related Commands

Command	Description
mpls traffic-eng reoptimize (EXEC mode)	Reoptimizes all traffic engineering tunnels immediately.
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.

mpls traffic-eng reoptimize timers frequency

To control the frequency with which tunnels with established label-switched paths (LSPs) are checked for better LSPs, use the **mpls traffic-eng reoptimize timers frequency** configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng reoptimize timers frequency *seconds*

no mpls traffic-eng reoptimize timers frequency

Syntax Description	*seconds*	Sets the frequency of reoptimization, in seconds. A value of 0 disables reoptimization.

Defaults

3600 seconds (1 hour), with a range of 0 to 604800 seconds (1 week).

Command Modes

Configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

A device with traffic engineering tunnels periodically examines tunnels with established LSPs to see 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 old, inferior LSP with the new, better LSP.

Examples

In the following example, the reoptimization frequency is set to 1 day:

```
Router(config)# mpls traffic-eng reoptimize timers frequency 86400
```

Related Commands

Command	Description
tunnel mpls traffic-eng path-option	If **lockdown** is specified, does not do a reoptimization check on this tunnel.
mpls traffic-eng reoptimize (EXEC mode)	Reoptimizes all traffic engineering tunnels immediately.

mpls traffic-eng router-id

To specify that the traffic engineering router identifier for the node is the IP address associated with a given interface, use the **mpls traffic-eng router-id** router configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng router-id *interface-name*

no traffic-eng router-id

Syntax Description

interface-name	Interface whose primary IP address is the router's identifier.

Defaults

No default behavior or values.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

This router's identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the destination node's traffic engineering router identifier, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.

Examples

In the following example, the traffic engineering router identifier is specified as the IP address associated with interface Loopback0:

```
Router(config-router)# mpls traffic-eng router-id Loopback0
```

Related Commands

Command	Description
mpls traffic-eng	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.

mpls traffic-eng signaling advertise implicit-null

To use MPLS encoding for the implicit-null label in signaling messages sent to neighbors that match the specified access list, use the **mpls traffic-eng signalling advertise implicit-null** configuration command. Use the **no** form of this command to disable this feature.

> **mpls traffic-eng signalling advertise implicit-null** [*aclname* | *aclnum*]

> **no mpls traffic-eng signalling advertise implicit-null**

Syntax Description		
	aclname	Name of the access list.
	aclnum	Number of the access list.

Defaults Use the Cisco encoding for the implicit-null label in signaling messages.

Command Modes Configuration

Command History	Release	Modification
	12.0(5)ST	This command was introduced.

Examples In the following example, the router is configured to use MPLS encoding for the implicit-null label when it sends signaling messages to certain peers:

```
Router(config)# mpls traffic-eng signalling advertise implicit-null
```

mpls traffic-eng tunnels (configuration)

To enable MPLS traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description   This command has no arguments or keywords.

Defaults   The feature is disabled.

Command Modes   Configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines   This command enables MPLS traffic engineering on a device. For you to use the feature, MPLS traffic engineering must also be enabled on the desired interfaces.

Examples   In the following example, MPLS traffic engineering tunnel signaling is turned on:

```
Router(config)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

mpls traffic-eng tunnels (interface)

To enable MPLS traffic engineering tunnel signaling on an interface (assuming that it is enabled on the device), use the **mpls traffic-eng tunnels** interface configuration command. Use the **no** form of this command to disable this feature.

mpls traffic-eng tunnels

no mpls traffic-eng tunnels

Syntax Description   This command has no arguments or keywords.

Defaults   The feature is disabled on all interfaces.

Command Modes   Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines   To enable MPLS traffic engineering on the interface, MPLS traffic engineering must also be enabled on the device. An enabled interface has its resource information flooded into the appropriate IGP link state database and accepts traffic engineering tunnel signaling requests.

Examples   In the following example, MPLS traffic engineering is enabled on interface Ethernet0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# mpls traffic-eng tunnels
```

Related Commands

Command	Description
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.

next-address

To specify the next IP address in the explicit path, use the **next-address** IP explicit path configuration subcommand. Use the **no** form of this command to disable this feature.

> **next-address** *A.B.C.D*

> **no next-address** *A.B.C.D*

Syntax Description		
A.B.C.D	Next IP address in the explicit path.	

Defaults No default behavior or values.

Command Modes IP explicit path configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.

Examples In the following example, the number 60 is assigned to the IP explicit path, the path is enabled, and 3.3.27.3 is specified as the next IP address in the list of IP addresses:

```
Router(config)# ip explicit-path identifier 60 enable
Router(cfg-ip-expl-path)# next-address 3.3.27.3

Explicit Path identifier 60:
    1: next-address 3.3.27.3
Router(cfg-ip-exp1-path)#
```

Related Commands	Command	Description
	append-after	Similar to the **index** subcommand, except that this command inserts the new path entry after the specified index number. Commands might be renumbered as a result.
	index	Inserts or modifies a path entry at a specified index.
	ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.
	list	Displays all or part of the explicit path(s).
	show ip explicit-paths	Displays configured IP explicit paths.

show ip explicit-paths

To display the configured IP explicit paths, use the **show ip explicit-paths** EXEC command. An IP explicit path is a list of IP addresses, each representing a node or link in the explicit path.

show ip explicit-paths [{ **name** *word* | **identifier** *number* }] [**detail**]

Syntax Description		
	name *word*	Name of the explicit path.
	identifier *number*	Number of the explicit path. Valid values are from 1 through 65535.
	detail	(Optional) Displays, in the long form, information about the configured IP explicit paths.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show ip explicit-paths** command:

```
Router# show ip explicit-paths

PATH 200 (strict source route, path complete, generation 6)
    1: next-address 3.3.28.3
    2: next-address 3.3.27.3
```

Table 1 describes the fields displayed in this example.

Table 1   show ip explicit-paths Field Descriptions

Field	Description
PATH	Path name or number, followed by the path status.
1: next-address	First IP address in the path.
2: next-address	Second IP address in the path.

Related Commands

Command	Description
append-after	Inserts a path entry after a specific index number. Commands might be renumbered as a result.
index	Inserts or modifies a path entry at a specific index.
ip explicit-path	Enters the subcommand mode for IP explicit paths so that you can create or modify the named path.

Command	Description
list	Displays all or part of the explicit path(s).
next-address	Specifies the next IP address in the explicit path.

show ip ospf database opaque-area

To display lists of information related to traffic engineering opaque link-state advertisements (LSAs), also known as Type-10 opaque link area link states, use the **show ip ospf database opaque-area** EXEC command.

show ip ospf database opaque-area

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.0(8)S	This command was introduced.

Examples   The following is sample output from the **show ip ospf database opaque-area** command:

```
Router# show ip ospf database opaque-area

OSPF Router with ID (25.3.3.3) (Process ID 1)

            Type-10 Opaque Link Area Link States (Area 0)

  LS age: 12
  Options: (No TOS-capability, DC)
  LS Type: Opaque Area Link
  Link State ID: 1.0.0.0
  Opaque Type: 1
  Opaque ID: 0
  Advertising Router: 24.8.8.8
  LS Seq Number: 80000004
  Checksum: 0xD423
  Length: 132
  Fragment number : 0

    MPLS TE router ID: 24.8.8.8

    Link connected to Point-to-Point network
      Link ID : 26.2.2.2

      Interface Address : 198.1.1.1
```

Table 2 describes the fields displayed in this example.

Table 2   show ip ospf database opaque-area Field Descriptions

Field	Description
LS age	Link state age.
Options	Type of service options.
LS Type	Type of the link state.
Link State ID	Router ID number.
Opaque Type	Opaque link-state type.
Opaque ID	Opaque LSA ID number.
Advertising Router	Advertising router ID.
LS Seq Number	Link state sequence number that detects old or duplicate link state advertisements.
Checksum	Fletcher checksum of the complete contents of the link state advertisement.
Length	Length, in bytes, of the link state advertisement.
Fragment number	Arbitrary value used to maintain multiple traffic engineering LSAs.
MPLS TE router ID	Unique MPLS traffic engineering ID.
Link ID	Index of the link being described.
Interface Address	Address of the interface.

Related Commands

Command	Description
mpls traffic-eng area	Configures a router running OSPF MPLS to flood traffic engineering for an indicated OSPF area.
mpls traffic-eng router-id	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.
show ip ospf mpls traffic-eng	Provides information about the links available on the local router for traffic engineering.

show ip ospf mpls traffic-eng

To display information about the links available on the local router for traffic engineering, use the **show ip ospf mpls traffic-eng** EXEC command.

show ip ospf [**process-id** [**area-id**]] **mpls traffic-eng** [**link**] | [**fragment**]

Syntax Description

process-id	(Optional) Internal identification number that is assigned locally when the OSPF routing process is enabled. The value can be any positive integer.
area-id	(Optional) Area number associated with the OSPF
link	Provides detailed information about the links over which traffic engineering is supported on the local router.
fragment	Provides detailed information about the traffic engineering fragments on the local router.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
Release 12.0S	This command was introduced.

Examples   The following is sample output from the **show ip ospf mpls traffic-eng** command:

```
router# show ip ospf mpls traffic-eng link

OSPF Router with ID (23.0.0.1) (Process ID 1)

  Area 0 has 2 MPLS TE links. Area instance is 14.

  Links in hash bucket 8.
    Link is associated with fragment 1. Link instance is 14
      Link connected to Point-to-Point network
      Link ID :197.0.0.1
      Interface Address :66.0.0.1
      Neighbor Address :66.0.0.2
      Admin Metric :97
      Maximum bandwidth :128000
      Maximum reservable bandwidth :250000
      Number of Priority :8
      Priority 0 :250000     Priority 1 :250000
      Priority 2 :250000     Priority 3 :250000
      Priority 4 :250000     Priority 5 :250000
      Priority 6 :250000     Priority 7 :212500
      Affinity Bit :0x0
    Link is associated with fragment 0. Link instance is 14
      Link connected to Broadcast network
      Link ID :195.1.1.2
      Interface Address :195.1.1.1
      Neighbor Address :195.1.1.2
      Admin Metric :10
      Maximum bandwidth :1250000
      Maximum reservable bandwidth :2500000
      Number of Priority :8
      Priority 0 :2500000    Priority 1 :2500000
      Priority 2 :2500000    Priority 3 :2500000
      Priority 4 :2500000    Priority 5 :2500000
      Priority 6 :2500000    Priority 7 :2500000
      Affinity Bit :0x0
```

Table 3 describes the fields displayed in this example.

Table 3   show ip ospf mpls traffic-eng Field Descriptions

Field	Description
OSPF Router with ID	Router identification number.
Process ID	OSPF process identification.
Area instance	Number of times traffic engineering information or any link changed.
Link instance	Number of times any link changed.
Link ID	Link state ID.
Interface Address	Local IP address on the link.
Neighbor Address	IP address that is on the remote end of the link.
Admin Metric	Traffic engineering link metric.
Maximum bandwidth	Bandwidth set by the **bandwidth interface** command.
Maximum reservable bandwidth	Bandwidth available for traffic engineering on this link. This value is set in the **ip rsvp** interface command.

Table 3   show ip ospf mpls traffic-eng Field Descriptions (continued)

Field	Description
Number of priority	Number of priorities that are supported.
Priority	Bandwidth, in bytes per second, that is available for traffic engineering at certain priorities.
Affinity Bit	Affinity bits (color) assigned to the link.

show ip rsvp host

To display RSVP terminal point information for receivers or senders, use the **show ip rsvp host** EXEC command.

show ip rsvp host { **senders** | **receivers**} [*hostname* | *A.B.C.D*]

Syntax Description		
senders	Displays information for senders.	
receivers	Displays information for receivers.	
hostname	Restricts the display to sessions with *hostname* as their destination.	
A.B.C.D	Restricts the display to sessions with the specified IP address as their destination.	

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show ip rsvp host receivers** command:

```
Router# show ip rsvp host receivers

To            From          Pro DPort Sport Next Hop     I/F   Fi Serv BPS Bytes
10.0.0.11     10.1.0.4      0   10011 1                        SE LOAD 100K  1K
```

Table 4 describes the fields displayed in this example.

Table 4   show ip rsvp host Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code.
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (wild card, shared explicit, or fixed).
Serv	Service (RATE or LOAD).

Table 4   show ip rsvp host Field Descriptions (continued)

Field	Description
BPS	Reservation rate, in bits per second.
Bytes	Bytes of requested burst size.

Related Commands

Command	Description
show ip rsvp request	Shows the RSVP reservations currently being requested upstream for a specified interface or all interfaces.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP-related sender information currently in the database.

show isis database verbose

To display more information about the database, use the **show isis database verbose** EXEC command.

> **show isis database verbose**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show isis database verbose** command:

```
Router# show isis database verbose

IS-IS Level-1 Link State Database
LSPID               LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
dtp-5.00-00         * 0x000000E6  0xC9BB        1042              0/0/0
  Area Address:49.0001
  NLPID:       0xCC
  Hostname:dtp-5
  Router ID:   5.5.5.5
  IP Address:  172.21.39.5
  Metric:10         IP 172.21.39.0/24
dtp-5.00-01         * 0x000000E7  0xAB36        1065              0/0/0
  Metric:10         IS-Extended dtp-5.01
    Affinity:0x00000000
    Interface IP Address:172.21.39.5
    Physical BW:10000000 bits/sec
    Reservable BW:1166000 bits/sec
    BW Unreserved[0]: 1166000 bits/sec, BW Unreserved[1]: 1166000 bits/sec
    BW Unreserved[2]: 1166000 bits/sec, BW Unreserved[3]: 1166000 bits/sec
    BW Unreserved[4]: 1166000 bits/sec, BW Unreserved[5]: 1166000 bits/sec
    BW Unreserved[6]: 1166000 bits/sec, BW Unreserved[7]: 1153000 bits/sec
  Metric:0          ES dtp-5
```

Table 5 describes the fields displayed in this example.

Table 5   show isis database verbose Field Descriptions

Field	Description
LSPID	LSP identifier.
	The first six octets form the System ID of the router that originated the link-state packet (LSP).
	The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. This is similar to a router LSA in OSPF; the LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP that describes all systems attached to that LAN.
	The last octet is the LSP number. If all the data cannot fit into a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the system issuing this command originated the LSP.
LSP Seq Num	LSP sequence number that allows other systems to determine if they received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time that the LSP remains valid, in seconds. An LSP holdtime of zero indicates that this LSP was purged and is being removed from all routers' link state databases (LSDBs). The value indicates how long the purged LSP will stay in the LSDB before it is completely removed.
ATT	Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1 routers use the Attach bit to find the closest Level 2 router. They install a default route to the closest Level 2 router.
P	P bit. This bit detects if the IS can repair area partitions. Cisco and other vendors do not support area partition repair.
OL	Overload bit. This bit determines if the IS is congested. If the overload bit is set, other routers do not use this system as a transit router when they calculate routes. Only packets for destinations directly connected to the overloaded router are sent to this router.
Area Address	Reachable area addresses from the router. For Level-1 LSPs, these are the area addresses configured manually on the originating router. For Level-2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID	Network Layer Protocol identifier.
Hostname	Host name of the node.
Router ID	Traffic engineering router identifier for the node.
IP Address	IPv4 address for the interface.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a connectionless network service (CLNS) prefix).
Affinity	Link attribute flags that are being flooded.

Table 5   show isis database verbose Field Descriptions (continued)

Field	Description
Physical BW	Link bandwidth capacity, in bits per second.
Reservable BW	Amount of reservable bandwidth on this link.
BW Unreserved	Amount of bandwidth that is available for reservation.

Related Commands

Command	Description
show isis mpls traffic-eng adjacency-log	Displays a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes.
show isis mpls traffic-eng advertisements	Displays the last flooded record from MPLS traffic engineering.
show isis mpls traffic-eng tunnel	Displays information about tunnels considered in the IS-IS next hop calculation.

show isis mpls traffic-eng adjacency-log

To display a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes, use the **show isis mpls traffic-eng adjacency-log** EXEC command.

show isis mpls traffic-eng adjacency-log

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show isis mpls traffic-eng adjacency-log** command:

```
Router# show isis mpls traffic-eng adjacency-log

IS-IS RRR log
When       Neighbor ID       IP Address       Interface Status Level
04:52:52   0000.0024.0004.02  0.0.0.0          Et0/2     Up     level-1
04:52:50   0000.0026.0001.00  170.1.1.2        PO1/0/0   Up     level-1
04:52:37   0000.0024.0004.02  0.0.0.0          Et0/2     Up     level-1
```

Table 6 describes the fields displayed in this example.

Table 6   show isis mpls traffic-eng adjacency-log Field Descriptions

Field	Description
When	Amount of time since the entry was recorded in the log.
Neighbor ID	Identification value of the neighbor.
IP Address	Neighbor IPv4 address.
Interface	Interface from which a neighbor is learned.
Status	Up (active) or Down (disconnected).
Level	Routing level.

Related Commands

Command	Description
show isis mpls traffic-eng advertisements	Displays the last flooded record from MPLS traffic engineering.

show isis mpls traffic-eng advertisements

To display the last flooded record from MPLS traffic engineering, use the **show isis mpls traffic-eng advertisements** EXEC command.

show isis mpls traffic-eng advertisements

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show isis mpls traffic-eng advertisements** command:

```
Router# show isis mpls traffic-eng advertisements

System ID:dtp-5.00
  Router ID:5.5.5.5
  Link Count:1
    Link[1]
      Neighbor System ID:dtp-5.01 (broadcast link)
      Interface IP address:172.21.39.5
      Neighbor IP Address:0.0.0.0
      Admin. Weight:10
      Physical BW:10000000 bits/sec
      Reservable BW:1166000 bits/sec
      BW unreserved[0]:1166000 bits/sec, BW unreserved[1]:1166000 bits/sec
      BW unreserved[2]:1166000 bits/sec, BW unreserved[3]:1166000 bits/sec
      BW unreserved[
4]:1166000 bits/sec, BW unreserved[5]:1166000 bits/sec
      BW unreserved[6]:1166000 bits/sec, BW unreserved[7]:1153000 bits/sec
      Affinity Bits:0x00000000
```

Table 7 describes the fields displayed in this example.

Table 7   show isis mpls traffic-eng advertisements Field Descriptions

Field	Description
System ID	Identification value for the local system in the area.
Router ID	MPLS traffic engineering router ID.
Link Count	Number of links that MPLS traffic engineering advertised.
Neighbor System ID	Identification value for the remote system in an area.

Table 7   show isis mpls traffic-eng advertisements Field Descriptions (continued)

Field	Description
Interface IP address	IPv4 address of the interface.
Neighbor IP Address	IPv4 address of the neighbor.
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link bandwidth capacity, in bits per second.
Reservable BW	Amount of reservable bandwidth on this link.
BW unreserved	Amount of bandwidth that is available for reservation.
Affinity Bits	Link attribute flags being flooded.

Related Commands

Command	Description
show isis mpls traffic-eng adjacency-log	Displays a log of 20 entries of MPLS traffic engineering IS-IS adjacency changes.

show isis mpls traffic-eng tunnel

To display information about tunnels considered in the IS-IS next hop calculation, use the **show isis mpls traffic-eng tunnel** EXEC command.

show isis mpls traffic-eng tunnel

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

EXEC

Command History

Release	Modification
12.0(5)	This command was introduced.

Examples

The following is sample output from the **show isis mpls traffic-eng tunnel** command:

```
Router# show isis mpls traffic-eng tunnel

Station Id          Tunnel Name   Bandwidth   Nexthop      Metric   Mode
kangpa-router1.00   Tunnel1022    3333        2.2.2.2      -3       Relative
                    Tunnel1021    10000       2.2.2.2      11       Absolute
tomklong-route.00   Tunnel1031    10000       3.3.3.3      -1       Relative
                    Tunnel1032    10000       3.3.3.3
```

Table 8 describes the fields displayed in this example.

Table 8   show isis mpls traffic-eng tunnel Field Descriptions

Field	Description
Station Id	Name or system ID of the MPLS traffic engineering tail-end router.
Tunnel Name	Name of the MPLS traffic engineering tunnel interface.
Bandwidth	MPLS traffic engineering tunnel's specified bandwidth.
Nexthop	MPLS traffic engineering tunnel's destination IP address.
Metric	MPLS traffic engineering tunnel's metric.
Mode	MPLS traffic engineering tunnel's metric mode. It can be relative or absolute.

Related Commands

Command	Description
show mpls traffic-eng autoroute	Shows tunnels that are announced to IGP, including interface, destination, and bandwidth.

show mpls traffic-eng autoroute

To show tunnels that are announced to the Interior Gateway Protocol (IGP), including interface, destination, and bandwidth, use the **show mpls traffic-eng autoroute** EXEC command.

show mpls traffic-eng autoroute

Syntax Description	This command has no arguments or keywords.

Defaults	No default behavior or values.

Command Modes	EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

The enhanced shortest path first (SPF) calculation of the IGP has been modified so that it uses traffic engineering tunnels. This command shows which tunnels IGP is currently using in its enhanced SPF calculation (that is, which tunnels are up and have autoroute configured).

Examples

The following is sample output from the **show mpls traffic-eng autoroute** command.

Note that the tunnels are organized by destination. All tunnels to a destination carry a share of the traffic tunneled to that destination.

```
Router# show mpls traffic-eng autoroute

MPLS TE autorouting enabled
  destination 0002.0002.0002.00 has 2 tunnels
    Tunnel1021 (traffic share 10000, nexthop 2.2.2.2, absolute metric 11)
    Tunnel1022 (traffic share 3333, nexthop 2.2.2.2, relative metric -3)
  destination 0003.0003.0003.00 has 2 tunnels
    Tunnel1032 (traffic share 10000, nexthop 3.3.3.3)
    Tunnel1031 (traffic share 10000, nexthop 3.3.3.3, relative metric -1)
```

Table 9 describes the fields displayed in this example.

Table 9   show mpls traffic-eng autoroute Field Descriptions

Field	Description
MPLS TE autorouting enabled	IGP automatically routes traffic into tunnels.
destination	MPLS traffic engineering tail-end router system ID.

Table 9   show mpls traffic-eng autoroute Field Descriptions (continued)

Field	Description
traffic share	A factor based on bandwidth, indicating how much traffic this tunnel should carry, relative to other tunnels, to the same destination. If two tunnels go to a single destination, one with a traffic share of 200 and the other with a traffic share of 100, the first tunnel carries two thirds of the traffic.
nexthop	MPLS traffic engineering tunnel's tail-end IP address.
absolute metric	MPLS traffic engineering tunnel's metric with mode absolute.
relative metric	MPLS traffic engineering tunnel's metric with mode relative.

Related Commands

Command	Description
show isis mpls traffic-eng tunnel	Displays information about tunnels considered in the IS-IS next hop calculation.
tunnel mpls traffic-eng autoroute announce	Causes the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.
tunnel mpls traffic-eng autoroute metric	Specifies the MPLS traffic engineering tunnel metric that the IGP enhanced SPF calculation will use.

show mpls traffic-eng link-management admission-control

To show which tunnels were admitted locally and their parameters (such as, priority, bandwidth, incoming and outgoing interface, and state), use the **show mpls traffic-eng link-management admission-control** EXEC command.

show mpls traffic-eng link-management admission-control [*interface-name*]

Syntax Description

interface-name	(Optional) Shows only tunnels that were admitted on the specified interface.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed. The BW field now shows bandwidth in kilobits per second, and it is followed by the status (reserved or held) of the bandwidth.

Examples

The following is sample output from the **show mpls traffic-eng link-management admission-control** command:

```
Router2# show mpls traffic-eng link-management admission-control

System Information::
    Tunnels Count:      4
    Tunnels Selected:   4
TUNNEL ID           UP IF      DOWN IF   PRIORITY STATE          BW (kbps)
10.106.0.6 1000_1   AT1/0.2    -         0/0      Resv Admitted  0
10.106.0.6 2000_1   Et4/0/1    -         1/1      Resv Admitted  0
10.106.0.6 1_2      Et4/0/1    Et4/0/2   1/1      Resv Admitted  3000        R
10.106.0.6 2_2      AT1/0.2    AT0/0.2   1/1      Resv Admitted  3000        R
```

Table 10 describes the fields displayed in this example.

Table 10   show mpls traffic-eng link-management admission-control Field Descriptions

Field	Description
Tunnels Count	Total number of tunnels admitted.
Tunnels Selected	Number of tunnels to be displayed.
TUNNEL ID	Tunnel identification.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.

Table 10   show mpls traffic-eng link-management admission-control Field Descriptions

Field	Description
PRIORITY	Tunnel's setup priority followed by the hold priority.
STATE	Tunnel's admission status.
BW (kbps)	Bandwidth of the tunnel, in kilobits per second. If an "R" follows the bandwidth number, the bandwidth is reserved. If an "H" follows the bandwidth number, the bandwidth is temporarily being held for a path message.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Shows local link information that MPLS traffic engineering link management is currently flooding into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.
show mpls traffic-eng link-management igp-neighbors	Shows Interior Gateway Protocol (IGP) neighbors.
show mpls traffic-eng link-management interfaces	Shows per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Shows a summary of link management information.

show mpls traffic-eng link-management advertisements

To show local link information that MPLS traffic engineering link management is currently flooding into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** EXEC command.

show mpls traffic-eng link-management advertisements

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed.

Examples   The following is sample output from the **show mpls traffic-eng link-management advertisements** command:

```
Router1# show mpls traffic-eng link-management advertisements

Flooding Status:      ready
Configured Areas:     1
IGP Area[1] ID:: isis level-1
  System Information::
    Flooding Protocol:   ISIS
  Header Information::
    IGP System ID:        0001.0000.0001.00
    MPLS TE Router ID:    10.106.0.6
    Flooded Links:        1
  Link ID:: 0
    Link IP Address:      10.1.0.6
    IGP Neighbor:         ID 0001.0000.0001.02
    Admin. Weight:        10
    Physical Bandwidth:   10000 kbits/sec
    Max Reservable BW:    5000 kbits/sec
    Downstream::
      Reservable Bandwidth[0]:      5000 kbits/sec
      Reservable Bandwidth[1]:      2000 kbits/sec
      Reservable Bandwidth[2]:      2000 kbits/sec
      Reservable Bandwidth[3]:      2000 kbits/sec
      Reservable Bandwidth[4]:      2000 kbits/sec
      Reservable Bandwidth[5]:      2000 kbits/sec
      Reservable Bandwidth[6]:      2000 kbits/sec
      Reservable Bandwidth[7]:      2000 kbits/sec
    Attribute Flags:      0x00000000
```

Table 11 describes the fields displayed in this example.

Table 11   show mpls traffic-eng link-management advertisements Field Descriptions

Field	Description
Flooding Status	Status of the link management flooding system.
Configured Areas	Number of the IGP areas configured.
IGP Area [1] ID	Name of the first IGP area.
Flooding Protocol	IGP that is flooding information for this area.
IGP System ID	Identification that IGP flooding uses in this area to identify this node.
MPLS TE Router ID	MPLS traffic engineering router ID.
Flooded Links	Number of links that are flooded in this area.
Link ID	Index of the link that is being described.
Link IP Address	Local IP address of this link.
IGP Neighbor	IGP neighbor on this link.
Admin. Weight	Administrative weight associated with this link.
Physical Bandwidth	Link bandwidth capacity, in kilobits per second.
Max Reservable BW	Amount of reservable bandwidth on this link.
Reservable Bandwidth	Amount of bandwidth that is available for reservation.
Attribute Flags	Link's attribute flags being flooded.

Related Commands

Command	Description
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.
show mpls traffic-eng link-management igp-neighbors	Shows IGP neighbors.
show mpls traffic-eng link-management interfaces	Shows per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Shows a summary of link management information.

show mpls traffic-eng link-management bandwidth-allocation

To show current local link information, use the **show mpls traffic-eng link-management bandwidth-allocation** EXEC command.

show mpls traffic-eng link-management bandwidth-allocation [*interface-name*]

Syntax Description		
	interface-name	(Optional) Shows only tunnels that were admitted on the specified interface.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed.

Usage Guidelines   Advertised information might differ from the current information, depending on how flooding was configured.

Examples   The following is sample output from the **show mpls traffic-eng link-management bandwidth-allocation** command:

```
Router1# show mpls traffic-eng link-management bandwidth-allocation Et4/0/1

System Information::
    Links Count:          2
    Bandwidth Hold Time: max. 15 seconds
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      BW Descriptors:      1
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      Up Thresholds:       15 30 45 60 75 80 85 90 95 96 97 98 99 100 (default)
      Down Thresholds:     100 99 98 97 96 95 90 85 80 75 60 45 30 15 (default)
    Downstream Bandwidth Information (kbits/sec):
      KEEP PRIORITY     BW HELD  BW TOTAL HELD   BW LOCKED  BW TOTAL LOCKED
                  0           0              0           0                0
                  1           0              0        3000             3000
                  2           0              0           0             3000
                  3           0              0           0             3000
                  4           0              0           0             3000
                  5           0              0           0             3000
                  6           0              0           0             3000
                  7           0              0           0             3000
```

Table 12 describes the fields displayed in this example.

Table 12   show mpls traffic-eng link-management bandwidth-allocation Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Bandwidth Hold Time	Amount of time that bandwidth can be held.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Link bandwidth capacity, in bits per second.
Max Reservable BW	Amount of reservable bandwidth on this link.
BW Descriptors	Number of bandwidth allocations on this link.
MPLS TE Link State	Status of the link's MPLS traffic engineering-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.
Up Thresholds	Link's bandwidth thresholds for allocations.
Down Thresholds	Link's bandwidth thresholds for deallocations.
KEEP PRIORITY	Priority levels for the link's bandwidth allocations.
BW HELD	Amount of bandwidth, in kilobits per second temporarily held at this priority for path messages.

Table 12   show mpls traffic-eng link-management bandwidth-allocation Field Descriptions

Field	Description
BW TOTAL HELD	Bandwidth held at this priority and those above it.
BW LOCKED	Amount of bandwidth reserved at this priority.
BW TOTAL LOCKED	Bandwidth locked at this priority and those above it.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management igp-neighbors	Shows IGP neighbors.
show mpls traffic-eng link-management interfaces	Shows per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Shows a summary of link management information.

show mpls traffic-eng link-management igp-neighbors

To show Interior Gateway Protocol (IGP) neighbors, use the **show mpls traffic-eng link-management igp-neighbors** EXEC command.

> **show mpls traffic-eng link-management igp-neighbors** [{ *igp-id* { **isis** *isis-address* | **ospf** *ospf-id* } | **ip** *A.B.C.D* }]

Syntax Description

igp-id	Shows the IGP neighbors that are using a specified IGP identification.
isis *isis-address*	Displays the specified IS-IS neighbor when you display neighbors by IGP ID.
ospf *ospf-id*	Displays the specified OSPF neighbor when you display neighbors by IGP ID.
ip *A.B.C.D*	Shows the IGP neighbors that are using a specified IGP IP address.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show mpls traffic-eng link-management igp-neighbors** command:

```
Router# show mpls traffic-eng line-management igp-neighbors

Link ID::  Et0/2
    Neighbor ID:  0000.0024.0004.02 (area: isis level-1, IP: 0.0.0.0)
Link ID::  PO1/0/0
    Neighbor ID:  0000.0026.0001.00 (area: isis level-1, IP: 170.1.1.2)
```

Table 13 describes the fields displayed in this example.

Table 13   show mpls traffic-eng link-management igp-neighbors Field Descriptions

Field	Description
Link ID	Link by which the neighbor is reached.
Neighbor ID	IGP identification information for the neighbor.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.
show mpls traffic-eng link-management interfaces	Shows per-interface resource and configuration information.
show mpls traffic-eng link-management summary	Shows a summary of link management information.

show mpls traffic-eng link-management interfaces

To show interface resource and configuration information, use the **show mpls traffic-eng link-management interfaces** EXEC command.

show mpls traffic-eng link-management interfaces [*interface-name*]

Syntax Description

interface-name	(Optional) Displays information only for the specified interface.

Defaults

Displays resource and configuration information for all configured interfaces.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed.

Examples

The following is sample output from the **show mpls traffic-eng link-management interfaces** command:

```
Router1# show mpls traffic-eng link-management interfaces Et4/0/1

System Information::
    Links Count:          2
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
      IGP Neighbor:        ID 0001.0000.0001.02, IP 0.0.0.0 (Up)
    Flooding Status for each configured area [1]:
      IGP Area[1]: isis level-1: flooded
```

Table 14 describes the fields displayed in this example.

Table 14   show mpls traffic-eng link management interfaces Field Descriptions

Field	Description
Links Count	Number of links that were enabled for use with MPLS traffic engineering.
Link ID	Index of the link.
Physical Bandwidth	Link's bandwidth capacity, in kilobits per second.

Table 14   show mpls traffic-eng link management interfaces Field Descriptions (continued)

Field	Description
Max Reservable BW	Amount of reservable bandwidth on this link.
MPLS TE Link State	The status of the MPLS link.
Inbound Admission	Link admission policy for inbound tunnels.
Outbound Admission	Link admission policy for outbound tunnels.
Admin. Weight	Administrative weight associated with this link.
IGP Neighbor Count	Number of IGP neighbors directly reachable over this link.
IGP Neighbor	IGP neighbor on this link.
Flooding Status for each configured area	Flooding status for the specified configured area.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.
show mpls traffic-eng link-management igp-neighbors	Shows IGP neighbors.
show mpls traffic-eng link-management summary	Shows a summary of link management information.

show mpls traffic-eng link-management summary

To show a summary of link management information, use the **show mpls traffic-eng link-management summary** EXEC command.

show mpls traffic-eng link-management summary [*interface-name*]

Syntax Description		
interface-name		(Optional) Displays information only for the specified interface.

Defaults   No default behavior or values.

Command Modes   EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed.

Examples   The following is sample output from the **show mpls traffic-eng link-management summary** command:

```
Router1# show mpls traffic-eng link-management summary

System Information::
    Links Count:        2
    Flooding System:    enabled
IGP Area ID:: isis level-1
    Flooding Protocol:  ISIS
    Flooding Status:    data flooded
    Periodic Flooding:  enabled (every 180 seconds)
    Flooded Links:      1
    IGP System ID:      0001.0000.0001.00
    MPLS TE Router ID:  10.106.0.6
    IGP Neighbors:      1
Link ID:: Et4/0/1 (10.1.0.6)
    Link Status:
      Physical Bandwidth:  10000 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
      MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
      Inbound Admission:   reject-huge
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  1
Link ID:: AT0/0.2 (10.42.0.6)
    Link Status:
      Physical Bandwidth:  155520 kbits/sec
      Max Reservable BW:   5000 kbits/sec (reserved:0% in, 0% out)
      MPLS TE Link State:  MPLS TE on, RSVP on
      Inbound Admission:   allow-all
      Outbound Admission:  allow-if-room
      Admin. Weight:       10 (IGP)
      IGP Neighbor Count:  0
```

Table 15 describes the fields displayed in this example.

Table 15   show mpls traffic-eng link-management summary Field Descriptions

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Flooding System	Enable status of the MPLS traffic engineering flooding system.
IGP Area ID	Name of the IGP area being described.
Flooding Protocol	IGP being used to flood information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Number of links that were flooded.
IGP System ID	IGP for this node associated with this area.
MPLS TE Router ID	MPLS traffic engineering router ID for this node.
IGP Neighbors	Number of reachable IGP neighbors associated with this area.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Link bandwidth capacity, in kilobits per second.
Max Reservable BW	Amount of reservable bandwidth on this link.

Table 15   show mpls traffic-eng link-management summary Field Descriptions (continued)

Field	Description
MPLS TE Link State	Status of the link's MPLS traffic engineering-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.

Related Commands

Command	Description
show mpls traffic-eng link-management advertisements	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
show mpls traffic-eng link-management bandwidth-allocation	Shows current local link information.
show mpls traffic-eng link-management igp-neighbors	Shows IGP neighbors.
show mpls traffic-eng link-management interfaces	Shows per-interface resource and configuration information.

show mpls traffic-eng topology

To show the MPLS traffic engineering global topology currently known at this node, use the **show mpls traffic-eng topology** EXEC command.

show mpls traffic-eng topology [{ *A.B.C.D* | **igp-id** { **isis** *nsapaddr* | **ospf** *A.B.C.D* }] [**brief**]

Syntax Description

A.B.C.D	Node IP address (router identifier to interface address).
igp-id	Node IGP router identifier.
isis *nsapaddr*	Node router identification, if IS-IS is enabled.
ospf *A.B.C.D*	Node router identifier, if OSPF is enabled.
brief	(Optional) Brief form of the output; gives a less detailed version of the topology.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output changed.

Examples

The following is sample output from the **show mpls traffic-eng topology** command:

```
Router1# show mpls traffic-eng topology 10.106.0.6

IGP Id:0001.0000.0001.00, MPLS TE Id:10.106.0.6 Router Node  id 1
    link[0 ]:Nbr IGP Id:0001.0000.0001.02, nbr_node_id:3, gen:14
        frag_id 0, Intf Address:10.1.0.6
        admin_weight:10, attribute_flags:0x0
        physical_bw:10000 (kbps), max_reservable_bw:5000 (kbps)
             allocated_bw    reservable_bw       allocated_bw    reservable_bw
             -----------    -------------       -----------    -------------
        bw[0]:0             5000            bw[1]:3000          2000
        bw[2]:0             2000            bw[3]:0             2000
        bw[4]:0             2000            bw[5]:0             2000
        bw[6]:0             2000            bw[7]:0             2000
```

Table 16 describes the fields displayed in this example.

Table 16   show mpls traffic-eng topology Field Descriptions

Field	Description
IGP Id	Identification of the advertising router.
MPLS TE Id	MPLS traffic engineering node identifier.

Table 16   show mpls traffic-eng topology Field Descriptions (continued)

Field	Description
Nbr IGP Id	Neighbor IGP interface.
nbr_node_id	Neighbor IGP router identifier.
gen	Generation number of the link state packet. This internal number is incremented when any new link state packet is received.
frag_id	IGP LSA fragment identifier.
Intf Address	This link's interface address.
admin_weight	Cost of the link.
attribute_flags	The requirements on the attributes of the links that the traffic crosses.
physical_bw	Physical line rate.
max_reservable_bw	Maximum amount of bandwidth that you can reserve on a link.
allocated_bw	Amount of bandwidth allocated at that priority.
reservable_bw	Amount of available bandwidth reservable at that priority.

Related Commands

Command	Description
show mpls traffic-eng tunnels	Shows information about tunnels.

show mpls traffic-eng topology path

To show the properties of the best available path to a specified destination that satisfies certain constraints, use the **show mpls traffic-eng topology path** EXEC command. You specify the constraints in this command.

> **show mpls traffic-eng topology path** { *tunnel-interface* [**destination** *address*]
> | **destination** *address* }
> [**bandwidth** *value*] [**priority** *value* [*value*]]
> [**affinity** *value* [**mask** *mask*]]

Syntax Description

tunnel-interface	Name of an MPLS traffic engineering interface (for example, Tunnel1) from which default constraints should be copied.
destination *address*	(Optional) IP address specifying the path's destination.
bandwidth *value*	(Optional) Bandwidth constraint; the amount of available bandwidth that a suitable path requires. This overrides the bandwidth constraint obtained from the specified tunnel interface. You can specify any positive number.
priority *value* [*value*]	(Optional) Priority constraints. The setup and hold priorities used to acquire bandwidth along the path. If specified, this overrides the priority constraints obtained from the tunnel interface. Valid values are from 0 to 7.
affinity *value*	(Optional) Affinity constraints. The link attributes for which the path has an affinity. If specified, this overrides the affinity constraints obtained from the tunnel interface.
mask *mask*	(Optional) Affinity constraints. The mask associated with the affinity specification.

Defaults

The specified constraints override any constraints obtained from a reference tunnel.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples   The following is sample output from the **show mpls traffic-eng topology path** command:

```
Router1# show mpls traffic-eng topology path Tunnel1 bandwidth 1000

Query Parameters:
  Destination:10.112.0.12
    Bandwidth:1000
   Priorities:1 (setup), 1 (hold)
     Affinity:0x0 (value), 0xFFFF (mask)
Query Results:
  Min Bandwidth Along Path:2000 (kbps)
  Max Bandwidth Along Path:5000 (kbps)
  Hop  0:10.1.0.6        :affinity 00000000, bandwidth 2000 (kbps)
  Hop  1:10.1.0.10       :affinity 00000000, bandwidth 5000 (kbps)
  Hop  2:10.43.0.10      :affinity 00000000, bandwidth 2000 (kbps)
  Hop  3:10.112.0.12
Router1#
```

Table 17 describes the fields displayed in this example.

Table 17   show mpls traffic-eng topology path Field Descriptions

Field	Description
Destination	IP address of the path's destination.
Bandwidth	Amount of available bandwidth that a suitable path requires.
Priorities	Setup and hold priorities used to acquire bandwidth.
Affinity	Link attributes for which the path has an affinity.
Min Bandwidth Along Path	Minimum amount of bandwidth configured for a path.
Max Bandwidth Along Path	Maximum amount of bandwidth configured for a path.
Hop	Information about each link in the path.

show mpls traffic-eng tunnels

To show information about tunnels, use the **show mpls traffic-eng tunnels** EXEC command.

show mpls traffic-eng tunnels *tunnel_interface* [**brief**]

show mpls traffic-eng tunnels
    [**destination** *address*]
    [**source-id** {*num* | *ipaddress* | *ipaddress num* }]
    [**role** {**all** | **head** | **middle** | **tail** | **remote** }]
    [{ **up** | **down** }]
    [**name** *string*]
    [**suboptimal constraints** {**none** | **current** | **max** }]
    [{ [**interface in** *phys_intf*] [**interface out** *phys_intf*] | [**interface** *phys_intf*]}]
    [**brief**]

Syntax Description		
tunnel_interface	Displays information for the specified tunneling interface.
brief	(Optional) Displays the information in brief format.
destination *address*	(Optional) Restricts the display to tunnels destined to the specified IP address.
source-id	Restricts the display to tunnels with a matching source IP address and/or tunnel number.
num	Tunnel number.
ipaddress	Source IP address.
ipaddress num	Source IP address and tunnel number.
role	Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
all	Displays all tunnels.
head	Displays tunnels with their heads at this router.
middle	Displays tunnels with their midpoints at this router.
tail	Displays tunnels with their tails at this router.
remote	Displays tunnels with their heads at another router; this is a combination of **middle** and **tail**.
up	Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
down	Displays tunnels that are down.
name *string*	Displays tunnels with the specified name. The tunnel name is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel name is included in the signaling message so it is available at all hops.
suboptimal constraints none	Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the IGP's shortest path.
suboptimal constraints current	Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options. Selected tunnels would have a shorter path if they were reoptimized immediately.

suboptimal constraints max	Displays tunnels whose path metric is greater than the current shortest path, constrained by the tunnel's configured options, and considering only the network's capacity. Selected tunnels would have a shorter path if no other tunnels were consuming network resources.
interface in *phys_intf*	Displays tunnels that use the specified input interface.
interface out *phys_intf*	Displays tunnels that use the specified output interface.
interface *phys_intf*	Displays tunnels that use the specified interface as an input or output interface.
brief	Specifies one line per tunnel.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The new **brief** format includes input and output interface information. The **suboptimal** and **interface** keywords were added to the nonbrief format. The nonbrief, nonsummary formats each include the history of LSP selection.

Examples

The following is sample output from the **show mpls traffic-eng tunnels brief** command:

```
Router1# show mpls traffic-eng tunnels brief

Signalling Summary:
    LSP Tunnels Process:          running
    RSVP Process:                 running
    Forwarding:                   enabled
    Periodic reoptimization:      every 3600 seconds, next in 1706 seconds
TUNNEL NAME                      DESTINATION      UP IF      DOWN IF     STATE/PROT
Router1_t1                       10.112.0.12      -          Et4/0/1     up/up
tagsw-r11_t2                     10.112.0.12      -          unknown     up/down
tagsw-r11_t3                     10.112.0.12      -          unknown     admin-down
tagsw-r11_t1000                  10.110.0.10      -          unknown     up/down
tagsw-r11_t2000                  10.110.0.10      -          Et4/0/1     up/up
Displayed 5 (of 5) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Table 18 describes the fields displayed in this example.

Table 18   show mpls traffic-eng Field Descriptions

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the RSVP process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization.

Table 18   show mpls traffic-eng Field Descriptions (continued)

Field	Description
TUNNEL NAME	Name of the interface that is configured at the tunnel head.
DESTINATION	Identifier of the tail-end router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
STATE/PROT	For tunnel heads, admin-down or up. For nonheads, signaled.

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

show mpls traffic-eng tunnels summary

To show summary information about tunnels, use the **show mpls traffic-eng tunnels summary** EXEC command.

> **show mpls traffic-eng tunnels summary**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following is sample output from the **show mpls traffic-eng tunnels summary command:**

```
Router# show mpls traffic-eng tunnels summary

Signalling Summary:
    LSP Tunnels Process:            running
    RSVP Process:                   running
    Forwarding:                     enabled
    Head: 1 interfaces, 1 active signalling attempts, 1 established
          1 activations, 0 deactivations
    Midpoints: 0, Tails: 0
    Periodic reoptimization:        every 3600 seconds, next in 3436 seconds
```

Table 19 describes the fields displayed in this example.

Table 19   *show mpls traffic-eng tunnels summary Field Descriptions*

Field	Description
LSP Tunnels Process	MPLS traffic engineering has or has not been enabled.
RSVP Process	RSVP has or has not been enabled. (This feature is enabled as a consequence of MPLS traffic engineering being enabled.)
Forwarding	Indicates whether appropriate forwarding is enabled. (Appropriate forwarding on a router is CEF switching.)
Head	Summary information about tunnel heads at this device.
Interfaces	Number of MPLS traffic engineering tunnel interfaces.
Active signalling attempts	LSPs currently successfully signaled or in the process of being signaled.
Established	LSPs currently signaled.

Table 19   show mpls traffic-eng tunnels summary Field Descriptions (continued)

Field	Description
Activations	Signaling attempts initiated.
Deactivations	Signaling attempts terminated.
Periodic reoptimization	Frequency of periodic reoptimization and time until the next periodic reoptimization.

Related Commands

Command	Description
mpls traffic-eng reoptimize timers frequency	Controls the frequency with which tunnels with established LSPs are checked for better LSPs.
mpls traffic-eng tunnels (configuration)	Enables MPLS traffic engineering tunnel signaling on a device.
mpls traffic-eng tunnels (interface)	Enables MPLS traffic engineering tunnel signaling on an interface.

tunnel mode mpls traffic-eng

To set the mode of a tunnel to MPLS for traffic engineering, use the **tunnel mode mpls traffic-eng** interface configuration command. Use the **no** form of this command to disable this feature.

> **tunnel mode mpls traffic-eng**

> **no tunnel mode mpls traffic-eng**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines   This command specifies that the tunnel interface is for an MPLS traffic engineering tunnel and enables the various tunnel MPLS configuration options.

Examples   In the following example, the tunnel's mode is set to MPLS traffic engineering:

```
Router(config-if)# tunnel mode mpls traffic-eng
```

Related Commands

Command	Description
tunnel mpls traffic-eng affinity	Configures an affinity for an MPLS traffic engineering tunnel.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel in its enhanced SPF calculation (if the tunnel is up).
tunnel mpls traffic-eng bandwidth	Configures the bandwidth required for an MPLS traffic engineering tunnel.
tunnel mpls traffic-eng path-option	Configures a path option.
tunnel mpls traffic-eng priority	Configures setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng affinity

To configure an affinity (the properties the tunnel requires in its links) for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng affinity** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

no tunnel mpls traffic-eng affinity *properties* [**mask** *mask value*]

Syntax Description

properties	Attribute values required for links carrying this tunnel. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.
mask *mask value*	(Optional) Link attribute to be checked. A 32-bit decimal number. Valid values are from 0x0 to 0xFFFFFFFF, representing 32 attributes (bits), where the value of an attribute is 0 or 1.

Defaults

properties: 0X00000000
mask value: 0X0000FFFF

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

The affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, a link's attribute value or that bit is irrelevant. If a bit in the mask is 1, the link's attribute value and the tunnel's required affinity for that bit must match.

A tunnel can use a link if the tunnel affinity equals the link attributes and the tunnel affinity mask.

Any properties set to 1 in the affinity should also be 1 in the mask. In other words, affinity and mask should be set such that

```
tunnel_affinity = (tunnel_affinity and tunnel_affinity_mask)
```

Examples

In the following example, the tunnel's affinity is set:

```
Router(config-if)# tunnel mpls traffic-eng affinity 0x0101 mask 0x303
```

Related Commands

Command	Description
mpls traffic-eng attribute-flags	Sets the attributes for the interface.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute announce

To specify that the IGP should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng autoroute announce

no tunnel mpls traffic-eng autoroute announce

Syntax Description
This command has no arguments or keywords.

Defaults
The IGP does not use the tunnel in its enhanced SPF calculation.

Command Modes
Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines
Currently, the only way to forward traffic onto a tunnel is by enabling this feature or by explicitly configuring forwarding (for example, with an interface static route).

Examples
In the following example, the instruction is given that if this tunnel is up, the IGP should use the tunnel in its enhanced SPF calculation:

```
Router(config-if)# tunnel mpls traffic-eng autoroute announce
```

In the following example, the instruction is given that if the IGP is using this tunnel in its enhanced SPF calculation, the IGP should give it an absolute metric of 10:

```
Router(config-if)# tunnel mpls traffic-eng autoroute metric absolute 10
```

In the following example, the tunnel requires 100 Kbps per second of bandwidth:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 100
```

Related Commands

Command	Description
ip route	Establishes static routes.
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

tunnel mpls traffic-eng autoroute metric

To specify the MPLS traffic engineering tunnel metric that the IGP enhanced SPF calculation uses, use the **tunnel mpls traffic-eng autoroute metric** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng autoroute metric { **absolute** | **relative** } *value*

no tunnel mpls traffic-eng autoroute metric

Syntax Description

absolute	Absolute metric mode; you can enter a positive metric value.
relative	Relative metric mode; you can enter a positive, negative, or zero value.
value	The metric that the IGP enhanced SPF calculation uses. The **relative** value can be from –10 to 10.

Defaults

The default is metric relative 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples

The following example designates that the IGP enhanced SPF calculation will use MPLS traffic engineering tunnel metric negative 1:

```
Router(config-if)# tunnel mpls traffic-eng autoroute metric relative –1
```

Related Commands

Command	Description
show mpls traffic-eng autoroute	Shows the tunnels announced to IGP, including interface, destination, and bandwidth.
tunnel mpls traffic-eng autoroute announce	Instructs the IGP to use the tunnel (if it is up) in its enhanced SPF calculation.

tunnel mpls traffic-eng bandwidth

To configure the bandwidth required for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng bandwidth *bandwidth*

no tunnel mpls traffic-eng bandwidth *bandwidth*

Syntax Description	*bandwidth*	The bandwidth required for an MPLS traffic engineering tunnel. Bandwidth is specified in kilobits per second.

Defaults　　Default bandwidth is 0.

Command Modes　　Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Examples　　In the following example, the bandwidth required for an MPLS traffic engineering tunnel is 1000:

```
Router(config-if)# tunnel mpls traffic-eng bandwidth 1000 1Xwn
```

Related Commands

Command	Description
show mpls traffic-eng tunnels	Displays tunnel information.

tunnel mpls traffic-eng path-option

To configure a path option for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng path-option** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng path-option *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number* }} [**lockdown**]

no tunnel mpls traffic-eng path-option *number* {**dynamic** | **explicit** {**name** *path-name* | *path-number* }} [**lockdown**]

Syntax Description

number	When multiple path options are configured, lower numbered options are preferred.
dynamic	LSP's path is dynamically calculated.
explicit	LSP's path is an IP explicit path.
name *path-name*	Path name of the IP explicit path that the tunnel uses with this option.
path-number	Path number of the IP explicit path that the tunnel uses with this option.
lockdown	The LSP cannot be reoptimized.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

You can configure multiple path options for a single tunnel. For example, there can be several explicit path options and a dynamic option for one tunnel. Path setup preference is for lower (not higher) numbers, so option 1 is preferred.

Examples

In the following example, the tunnel is configured to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option 1 explicit name test
```

Related Commands

Command	Description
ip explicit-path	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.

Command	Description
show ip explicit-paths	Displays the configured IP explicit paths.
tunnel mpls traffic-eng priority	Configures the setup and reservation priority for an MPLS traffic engineering tunnel.

tunnel mpls traffic-eng priority

To configure the setup and reservation priority for an MPLS traffic engineering tunnel, use the **tunnel mpls traffic-eng priority** interface configuration command. Use the **no** form of this command to disable this feature.

tunnel mpls traffic-eng priority *setup-priority* [*hold-priority*]

no tunnel traffic-eng priority *setup-priority* [*hold-priority*]

Syntax Description

setup-priority	The priority used when signaling an LSP for this tunnel to determine what existing tunnels 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.
hold-priority	(Optional) The priority associated with an LSP for this tunnel 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.

Defaults

setup-priority: 7
hold-priority: The same value as the *setup* priority

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)S	This command was introduced.

Usage Guidelines

When an LSP is being signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs so that the new LSP can be admitted. (LSPs are preempted if that allows the new LSP to be admitted.)

In the above determination, the new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).

Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples

In the following example, a tunnel is configured with a setup and hold priority of 1.

```
Router(config-if)# tunnel mpls traffic-eng priority 1
```

Related Commands

Command	Description
tunnel mode mpls traffic-eng	Sets the mode of a tunnel to MPLS for traffic engineering.

Debug Commands

This section documents new or modified debug commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

- **debug ip ospf mpls traffic-eng advertisements**
- **debug isis mpls traffic-eng advertisements**
- **debug isis mpls traffic-eng events**
- **debug mpls traffic-eng areas**
- **debug mpls traffic-eng autoroute**
- **debug mpls traffic-eng link-management admission-control**
- **debug mpls traffic-eng link-management advertisements**
- **debug mpls traffic-eng link-management bandwidth-allocation**
- **debug mpls traffic-eng link-management errors**
- **debug mpls traffic-eng link-management events**
- **debug mpls traffic-eng link-management igp-neighbors**
- **debug mpls traffic-eng link-management links**
- **debug mpls traffic-eng link-management preemption**
- **debug mpls traffic-eng link-management routing**
- **debug mpls traffic-eng load-balancing**
- **debug mpls traffic-eng path**
- **debug mpls traffic-eng topology change**
- **debug mpls traffic-eng topology lsa**
- **debug mpls traffic-eng tunnels errors**
- **debug mpls traffic-eng tunnels events**
- **debug mpls traffic-eng tunnels labels**
- **debug mpls traffic-eng tunnels reoptimize**
- **debug mpls traffic-eng tunnels signalling**
- **debug mpls traffic-eng tunnels state**
- **debug mpls traffic-eng tunnels timers**

debug ip ospf mpls traffic-eng advertisements

To print information about traffic engineering advertisements in OSPF Link State Advertisement (LSA) messages, use the **debug ip ospf mpls traffic-eng advertisements** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug ip ospf mpls traffic-eng advertisements**

Syntax Description This command has no arguments or keywords

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples In the following example, information about traffic engineering advertisements is printed in OSPF LSA messages:

```
debug ip ospf mpls traffic-eng advertisements

OSPF:IGP delete router node 10.106.0.6 fragment 0 with 0 links
      TE Router ID 10.106.0.6
OSPF:IGP update router node 10.110.0.10 fragment 0 with 0 links
      TE Router ID 10.110.0.10
OSPF:MPLS announce router node 10.106.0.6 fragment 0 with 1 links
      Link connected to Point-to-Point network
      Link ID :10.110.0.10
      Interface Address :10.1.0.6
      Neighbor Address :10.1.0.10
      Admin Metric :10
      Maximum bandwidth :1250000
      Maximum reservable bandwidth :625000
      Number of Priority :8
      Priority 0 :625000      Priority 1 :625000
      Priority 2 :625000      Priority 3 :625000
      Priority 4 :625000      Priority 5 :625000
      Priority 6 :625000      Priority 7 :625000
      Affinity Bit :0x0
```

Table 20 describes the fields displayed in this example.

Table 20   debug ip ospf mpls traffic-eng advertisements Field Descriptions

Field	Description
Link ID	Index of the link being described.
Interface Address	Address of the interface.
Neighbor Address	Address of the neighbor.
Admin Metric	Administrative weight associated with this link.
Maximum bandwidth	Link's bandwidth capacity, in kilobits per second.
Maximum reservable bandwidth	Amount of reservable bandwidth on this link.
Number of Priority	Number of priority levels for which bandwidth is advertised.
Priority	Bandwidth available at indicated priority level.
Affinity Bit	Link's attribute flags that are being flooded.

debug isis mpls traffic-eng advertisements

To print information about traffic engineering advertisements in ISIS Link State Advertisement (LSA) messages, use the **debug isis mpls traffic-eng advertisements** EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug isis mpls traffic-eng advertisements**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples   In the following example, information about traffic engineering advertisements is printed in ISIS LSA messages:

```
debug isis mpls traffic-eng advertisements

System ID:Router1.00
  Router ID:10.106.0.6
  Link Count:1
    Link[1]
      Neighbor System ID:Router2.00 (P2P link)
      Interface IP address:10.42.0.6
      Neighbor IP Address:10.42.0.10
      Admin. Weight:10
      Physical BW:155520000 bits/sec
      Reservable BW:5000000 bits/sec
      BW unreserved[0]:2000000 bits/sec, BW unreserved[1]:100000 bits/sec
      BW unreserved[2]:100000 bits/sec, BW unreserved[3]:100000 bits/sec
      BW unreserved[4]:100000 bits/sec, BW unreserved[5]:100000 bits/sec
      BW unreserved[6]:100000 bits/sec, BW unreserved[7]:0 bits/sec
      Affinity Bits:0x00000000
```

Table 21 describes the fields displayed in this example.

Table 21   debug isis mpls traffic-eng advertisements Field Descriptions

Field	Description
System ID	Identification value for the local system in the area.
Router ID	MPLS traffic engineering router ID.
Link Count	Number of links that MPLS traffic engineering advertised.

Table 21   debug isis mpls traffic-eng advertisements Field Descriptions (continued)

Field	Description
Neighbor System ID	Identification value for the remote system in an area.
Interface IP address	IPv4 address of the interface.
Neighbor IP Address	IPv4 address of the neighbor.
Admin. Weight	Administrative weight associated with this link.
Physical BW	Link's bandwidth capacity, in bits per second.
Reservable BW	Amount of reservable bandwidth on this link.
BW unreserved	Amount of bandwidth that is available for reservation.
Affinity Bits	Link's attribute flags that are being flooded.

debug isis mpls traffic-eng events

To print information about traffic engineering-related ISIS events, use the **debug isis mpls traffic-eng events** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug isis mpls traffic-eng events**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples   In the following example, information is printed about traffic engineering-related ISIS events:

```
debug isis mpls traffic-eng events

ISIS-RRR:Send MPLS TE Et4/0/1 Router1.02 adjacency down:address 0.0.0.0
ISIS-RRR:Found interface address 10.1.0.6 Router1.02, building subtlv... 58 bytes
ISIS-RRR:Found interface address 10.42.0.6 Router2.00, building subtlv... 64 bytes
ISIS-RRR:Interface address 0.0.0.0 Router1.00 not found, not building subtlv
ISIS-RRR:LSP Router1.02 changed from 0x606BCD30
ISIS-RRR:Mark LSP Router1.02 changed because TLV contents different, code 16
ISIS-RRR:Received 1 MPLS TE links flood info for system id Router1.00
```

debug mpls traffic-eng areas

To print information about traffic engineering area configuration change events, use the **debug mpls traffic-eng areas** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng areas**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, information is printed about traffic engineering area configuration change events:

```
debug mpls traffic-eng areas

TE-AREAS:isis level-1:up event
TE-PCALC_LSA:isis level-1
```

debug mpls traffic-eng autoroute

To print information about automatic routing over traffic engineering tunnels, use the **debug mpls traffic-eng autoroute** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng autoroute**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, information is printed about automatic routing over traffic engineering tunnels:

```
debug mpls traffic-eng autoroute

TE-Auto:announcement that destination 0001.0000.0003.00 has 1 tunnels
    Tunnel1 (traffic share 333, nexthop 10.112.0.12)
```

debug mpls traffic-eng link-management admission-control

To print information about traffic engineering LSP admission control on traffic engineering interfaces, use the **debug mpls traffic-eng link-management admission-control** privileged EXEC command. To disable debugging output, use the **no** form of this command.

debug mpls traffic-eng link-management admission-control [**detail**] [*aclnum*]

no debug mpls traffic-eng link-management admission-control [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.
aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information only for those LSPs that match the access list.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the *aclnum* option were added.

Examples

In the following example, information is printed about traffic engineering LSP admission control on traffic engineering interfaces:

```
debug mpls traffic-eng link-management admission-control

TE-LM-ADMIT:tunnel 10.106.0.6 1_10002:created [total 4]
TE-LM-ADMIT:tunnel 10.106.0.6 1_10002: "None" -> "New"
TE-LM-ADMIT:tunnel 10.106.0.6 1_10002: "New" -> "Admitting 2nd Path Leg"
TE-LM-ADMIT:tunnel 10.106.0.6 1_10002: "Admitting 2nd Path Leg" -> "Path Admitted"
TE-LM-ADMIT:Admission control has granted Path query for 10.106.0.6 1_10002 (10.112.0.12)
on link Ethernet4/0/1 [reason 0]
TE-LM-ADMIT:tunnel 10.106.0.6 1_10002: "Path Admitted" -> "Admitting 1st Resv Leg"
TE-LM-ADMIT:tunnel 10.106.0.6 1_10002: "Admitting 1st Resv Leg" -> "Resv Admitted"
TE-LM-ADMIT:Admission control has granted Resv query for 10.106.0.6 1_10002 (10.112.0.12)
on link Ethernet4/0/1 [reason 0]
```

debug mpls traffic-eng link-management advertisements

To print information about resource advertisements for traffic engineering interfaces, use the **debug mpls traffic-eng link-management advertisements** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management advertisements** [**detail**] [*aclnum*]

Syntax Description

detail	(Optional) Prints detailed debugging information.
aclnum	(Optional) Uses the specified access list to filter the debugging information.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples   In the following example, detailed debugging information is printed about resource advertisements for traffic engineering interfaces:

```
debug mpls traffic-eng link-management advertisements detail

TE-LM-ADV:area isis level-1:IGP announcement:link Et4/0/1:info changed
TE-LM-ADV:area isis level-1:IGP msg:link Et4/0/1:includes subnet type (2), described nbrs
(1)
TE-LM-ADV:area isis level-1:IGP announcement:link Et4/0/1:info changed
TE-LM-ADV:area isis level-1:IGP msg:link Et4/0/1:includes subnet type (2), described nbrs
(1)
TE-LM-ADV:LSA:Flooding manager received message:link information change (Et4/0/1)
TE-LM-ADV:area isis level-1:*** Flooding node information ***
  System Information::
    Flooding Protocol:    ISIS
  Header Information::
    IGP System ID:        0001.0000.0001.00
    MPLS TE Router ID:    10.106.0.6
    Flooded Links:        1
  Link ID:: 0
    Link IP Address:      10.1.0.6
    IGP Neighbor:         ID 0001.0000.0001.02
    Admin. Weight:        10
    Physical Bandwidth:   10000 kbits/sec
    Max Reservable BW:    5000 kbits/sec
    Downstream::
      Reservable Bandwidth[0]:      5000 kbits/sec
      Reservable Bandwidth[1]:      2000 kbits/sec
      Reservable Bandwidth[2]:      2000 kbits/sec
      Reservable Bandwidth[3]:      2000 kbits/sec
      Reservable Bandwidth[4]:      2000 kbits/sec
      Reservable Bandwidth[5]:      2000 kbits/sec
      Reservable Bandwidth[6]:      2000 kbits/sec
Attribute Flags: 0x00000000
```

Table 22 describes the fields displayed in this example.

Table 22   debug isis mpls traffic-eng advertisements Field Descriptions

Field	Description
Flooding Protocol	IGB that is flooding information for this area.
IGP System ID	Identification that IGP flooding uses in this area to identify this node.
MPLS TE Router ID	MPLS traffic engineering router ID.
Flooded Links	Number of links that are flooded in this area.
Link ID	Index of the link that is being described.
Link IP Address	Local IP address of this link.
IGP Neighbor	IGP neighbor on this link.
Admin. Weight	Administrative weight associated with this link.
Physical Bandwidth	Link's bandwidth capacity, in kilobits per second.
Max Reservable BW	Maximum amount of bandwidth that is currently available for reservation at this priority.
Reservable Bandwidth	Amount of bandwidth that is available for reservation.
Attribute Flags	Link's attribute flags being flooded.

debug mpls traffic-eng link-management bandwidth-allocation

To print detailed information about bandwidth allocation for traffic engineering LSPs, use the **debug mpls traffic-eng link-management bandwidth-allocation** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management bandwidth-allocation** [**detail**] [*aclnum*]

Syntax Description

detail	(Optional) Prints detailed debugging information.
aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information only for those LSPs that match the access list.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the *aclnum* option were added.

Examples

In the following example, information is printed about bandwidth allocation for traffic engineering LSPs:

debug mpls traffic-eng link-management bandwidth-allocation

```
TE-LM-BW:tunnel 10.106.0.6 1_10002:requesting Downstream bw hold (3000000 bps [S]) on
link Et4/0/1
TE-LM-BW:tunnel 10.106.0.6 1_10002:Downstream bw hold request succeeded
TE-LM-BW:tunnel 10.106.0.6 1_10002:requesting Downstream bw lock (3000000 bps [S]) on
link Et4/0/1
TE-LM-BW:tunnel 10.106.0.6 1_10002:Downstream bw lock request succeeded _„Rs
```

Related Commands

Command	Description
debug mpls traffic-eng link-management admission-control	Prints information about traffic engineering LSP admission control on traffic engineering interfaces.
debug mpls traffic-eng link-management errors	Prints information about errors encountered during any traffic engineering link management procedure.

debug mpls traffic-eng link-management errors

To print information about errors encountered during any traffic engineering link management procedure, use the **debug mpls traffic-eng link-management errors** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management errors** [**detail**]

Syntax Description		
	detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, detailed debugging information is printed about errors encountered during a traffic engineering link management procedure:

```
debug mpls traffic-eng link-management errors detail
```

```
00:04:48 TE-LM-ROUTING: link Et1/1/1: neighbor 0010.0000.0012.01: add to IP peer db
failed
```

Related Commands

Command	Description
debug mpls traffic-eng link-management admission-control	Prints information about traffic engineering LSP admission control on traffic engineering interfaces.
debug mpls traffic-eng link-management advertisements	Prints information about resource advertisements for traffic engineering interfaces.
debug mpls traffic-eng link-management bandwidth-allocation	Prints information about bandwidth allocation for traffic engineering LSPs.
debug mpls traffic-eng link-management events	Prints information about traffic engineering link management system events.
debug mpls traffic-eng link-management igp-neighbors	Prints information about changes to the link management databases of IGP neighbors.
debug mpls traffic-eng link-management links	Prints information about traffic engineering link management interface events.

debug mpls traffic-eng link-management events

To print information about traffic engineering link management system events, use the **debug mpls traffic-eng link-management events** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management events** [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples

In the following example, detailed debugging information is printed about traffic engineering link management system events:

```
debug mpls traffic-eng link-management events detail

TE-LM-EVENTS:stopping MPLS TE Link Management process
TE-LM-EVENTS:MPLS TE Link Management process dying now
```

debug mpls traffic-eng link-management igp-neighbors

To print information about changes to the link management database of IGP neighbors, use the **debug mpls traffic eng link-management igp-neighbors** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management igp-neighbors** [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples

In the following example, detailed debugging information is printed about changes to the link management database of IGP neighbors:

```
debug mpls traffic-eng link-management igp-neighbors detail

TE-LM-NBR:link AT0/0.2:neighbor 0001.0000.0002.00:created (isis level-1, 10.42.0.10,
Up)[total 2]
```

Related Commands

Command	Description
debug mpls traffic-eng link-management events	Prints information about traffic engineering-related ISIS events.

debug mpls traffic-eng link-management links

To print information about traffic engineering link management interface events, use the **debug mpls traffic-eng link-management links** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management links** [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples

In the following example, detailed debugging information is printed about traffic engineering link management interface events:

```
debug mpls traffic-eng link-management links detail

TE-LM-LINKS:link AT0/0.2:RSVP enabled
TE-LM-LINKS:link AT0/0.2:increasing RSVP bandwidth from 0 to 5000000
TE-LM-LINKS:link AT0/0.2:created [total 2]
TE-LM-LINKS:Binding MPLS TE LM Admission Control as the RSVP Policy Server on ATM0/0.2
TE-LM-LINKS:Bind attempt succeeded
TE-LM-LINKS:link AT0/0.2:LSP tunnels enabled
```

debug mpls traffic-eng link-management preemption

To print information about traffic engineering LSP preemption, use the **debug mpls traffic-eng link-management preemption** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng link-management preemption** [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, detailed debugging information is printed about traffic engineering LSP preemption:

```
debug mpls traffic-eng link-management preemption detail

TE-LM-BW:preempting Downstream bandwidth, 1000000, for tunnel 10.106.0.6 2_2
TE-LM-BW:building preemption list to get bandwidth, 1000000, for tunnel 10.106.0.6 2_2
(priority 0)
TE-LM-BW:added bandwidth, 3000000, from tunnel 10.106.0.6 1_2 (pri 1) to preemption list
TE-LM-BW:preemption list build to get bw, 1000000, succeeded (3000000)
TE-LM-BW:preempting bandwidth, 1000000, using plist with 1 tunnels
TE-LM-BW:tunnel 10.106.0.6 1_2:being preempted on AT0/0.2 by 10.106.0.6 2_2
TE-LM-BW:preemption of Downstream bandwidth, 1000000, succeeded
```

debug mpls traffic-eng link-management routing

To print information about traffic engineering link management routing resolutions that can be performed to help RSVP interpret explicit route objects, use the **debug mpls traffic-eng link-management routing** privileged EXEC command. Use the **no** form of this command to disable debugging output.

[**no**] **debug mpls traffic-eng link-management routing** [**detail**]

Syntax Description	detail	(Optional) Prints detailed debugging information.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples

In the following example, detailed debugging information is printed about traffic engineering link management routing resolutions that can be performed to help RSVP interpret explicit route objects:

```
debug mpls traffic-eng link-management routing detail

TE-LM-ROUTING:route options to 10.42.0.10:building list (w/ nhop matching)
TE-LM-ROUTING:route options to 10.42.0.10:adding {AT0/0.2, 10.42.0.10}
TE-LM-ROUTING:route options to 10.42.0.10:completed list has 1 links
```

Related Commands

Command	Description
debug ip rsvp	Prints information about RSVP signaling events.

debug mpls traffic-eng load-balancing

To print information about unequal cost load balancing over traffic engineering tunnels, use the **debug mpls traffic-eng load-balancing** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng load-balancing**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples   In the following example, information is printed about unequal cost load balancing over traffic engineering tunnels:

```
debug mpls traffic-eng load-balancing

TE-Load:10.210.0.0/16, 2 routes, loadbalancing based on MPLS TE bandwidth
TE-Load:10.200.0.0/16, 2 routes, loadbalancing based on MPLS TE bandwidth
```

debug mpls traffic-eng path

To print information about traffic engineering path calculation, use the **debug mpls traffic-eng path** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng path** {*num* | **lookup** | **spf** | **verify**}

Syntax Description

num	Prints path calculation information only for the local tunneling interface with unit number *num*.
lookup	Prints information for path lookups.
spf	Prints information for shortest path first (SPF) calculations.
verify	Prints information for path verifications.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, information is printed about the calculation of the traffic engineering path:

```
debug mpls traffic-eng path lookup

TE-PCALC:Tunnel1000 Path Setup to 10.110.0.10:FULL_PATH
TE-PCALC:bw 0, min_bw 0, metric:0
TE-PCALC:setup_pri 0, hold_pri 0
TE-PCALC:affinity_bits 0x0, affinity_mask 0xFFFF
TE-PCALC_PATH:create_path_hoplist:ip addr 10.42.0.6 unknown.
```

debug mpls traffic-eng topology change

To print information about traffic engineering topology change events, use the **debug mpls traffic-eng topology change** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng topology change**

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples

In the following example, information is printed about traffic engineering topology change events:

```
debug mpls traffic-eng topology change

TE-PCALC_LSA:NODE_CHANGE_UPDATE isis level-1
        link flags:LINK_CHANGE_BW
        system_id:0001.0000.0001.00, my_ip_address:10.42.0.6
        nbr_system_id:0001.0000.0002.00, nbr_ip_address 10.42.0.10
```

debug mpls traffic-eng topology lsa

To print information about traffic engineering topology link state advertisement (LSA) events, use the **debug mpls traffic-eng topology lsa** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng topology lsa**

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.0(5)ST	This command was introduced.

Examples   In the following example, information is printed about traffic engineering topology LSA events:

```
debug mpls traffic-eng topology lsa

TE-PCALC_LSA:node_lsa_add:Received a LSA:flags 0x1 !

IGP Id:0001.0000.0001.00, MPLS TE Id:10.106.0.6 is VALID has 2 links (frag_id 0)
      link[0 ]:Nbr IGP Id:0001.0000.0001.02
          frag_id 0, Intf Address:0.0.0.0
          admin_weight:10, attribute_flags:0x0

      link[1 ]:Nbr IGP Id:0001.0000.0002.00
          frag_id 0, Intf Address:10.42.0.6, Nbr Intf Address:10.42.0.10
          admin_weight:100, attribute_flags:0x0
TE-PCALC_LSA:(isis level-1):Received lsa:

IGP Id:0001.0000.0001.00, MPLS TE Id:10.106.0.6 Router Node  id 8
      link[0 ]:Nbr IGP Id:0001.0000.0002.00, nbr_node_id:9, gen:114
          frag_id 0, Intf Address:10.42.0.6, Nbr Intf Address:10.42.0.10
          admin_weight:100, attribute_flags:0x0
          physical_bw:155520 (kbps), max_reservable_bw:5000 (kbps)
              allocated_bw   reservable_bw      allocated_bw   reservable_bw
              ------------   -------------      ------------   -------------
          bw[0]:0            5000           bw[1]:3000         2000
          bw[2]:0            2000           bw[3]:0            2000
          bw[4]:0            2000           bw[5]:0            2000
          bw[6]:0            2000           bw[7]:0            2000
```

debug mpls traffic-eng tunnels errors

To print information about errors encountered during any traffic engineering tunnel management procedure, use the **debug mpls traffic-eng tunnels errors** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels errors** [**detail**]

Syntax Description	**detail**	(Optional) Prints detailed debugging information.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced.

Examples   In the following example, detailed debugging information is printed about errors encountered during a traffic engineering tunnel management procedure:

```
debug mpls traffic-eng tunnels errors
```

```
00:04:14: LSP-TUNNEL-SIG: Tunnel10012[1]: path verification failed (unprotected) [Can't
use link 10.12.4.4 on node 10.0.0.4]
```

debug mpls traffic-eng tunnels events

To print information about traffic engineering tunnel management system events, use the **debug mpls traffic-eng tunnels events** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels events** [**detail**]

Syntax Description

detail	(Optional) Prints detailed debugging information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword was added.

Examples

In the following example, detailed debugging information is printed about traffic engineering tunnel management system events:

```
debug mpls traffic-eng tunnels events detail

LSP-TUNNEL:received event:interface admin. down [Ethernet4/0/1]
LSP-TUNNEL:posting action(s) to all-tunnels:
            check static LSPs
LSP-TUNNEL:scheduling pending actions on all-tunnels
LSP-TUNNEL:applying actions to all-tunnels, as follows:
            check static LSPs
```

debug mpls traffic-eng tunnels labels

To print information about MPLS label management for traffic engineering tunnels, use the **debug mpls traffic-eng tunnels labels** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels labels** [**detail**] [*aclnum*]

Syntax Description		
detail	(Optional) Prints detailed debugging information.	
aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information only about traffic engineering tunnels that match the access list.	

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the *aclnum* option were added.

Examples

In the following example, detailed debugging information is printed about MPLS label management for traffic engineering tunnels:

```
debug mpls traffic-eng tunnels labels detail

LSP-TUNNEL-LABELS:tunnel 10.106.0.6 1 [2]:fabric PROGRAM request
LSP-TUNNEL-LABELS:tunnel 10.106.0.6 1 [2]:programming label 16 on output interface
ATM0/0.2
LSP-TUNNEL-LABELS:descriptor 71FA64:continuing "Program" request
LSP-TUNNEL-LABELS:descriptor 71FA64:set "Interface Point Out State" to, allocated
LSP-TUNNEL-LABELS:# of resource points held for "default" interfaces:2
LSP-TUNNEL-LABELS:descriptor 71FA64:set "Fabric State" to, enabled
LSP-TUNNEL-LABELS:descriptor 71FA64:set "Fabric Kind" to, default (LFIB)
LSP-TUNNEL-LABELS:descriptor 71FA64:set "Fabric State" to, set
LSP-TUNNEL-LABELS:tunnel 10.106.0.6 1 [2]:fabric PROGRAM reply
```

To restrict output to information about a single tunnel, you can configure an access list and supply it to the debug command. Configure the access list as follows:

```
Router(config-ext-nacl)# permit udp host scr_address host dst_address eq tun intfc
```

For example, if tunnel 10012 has destination 10.0.0.11 and source 10.0.0.4, as determined by **show mpls traffic-eng tunnels**, the following access list could be configured and added to the debug command:

```
Router(config-ext-nacl)# permit udp host 10.0.0.4 10.0.0.11 eq 10012
```

debug mpls traffic-eng tunnels reoptimize

To print information about traffic engineering tunnel reoptimizations, use the **debug mpls traffic-eng tunnels reoptimize** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels reoptimize** [**detail**] [*aclnum*]

Syntax Description	**detail** — (Optional) Prints detailed debugging information.
	aclnum — (Optional) Uses the specified access list to filter the debugging information. Prints information about only those traffic engineering tunnel reoptimizations that match the access list.

Defaults   No default behavior or values.

Command Modes   Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the *aclnum* option were added.

Examples   In the following example, detailed debugging information is printed about traffic engineering tunnel reoptimizations that match access list number 101.

```
debug mpls traffic-eng tunnels reoptimize detail 101

LSP-TUNNEL-REOPT:Tunnel1 curr option 2 (0x6175CF8C), activate new option 2
LSP-TUNNEL-REOPT:Tunnel1 new path:option 2 [10002], weight 20
LSP-TUNNEL-REOPT:Tunnel1 old path:option 2 [2], weight 110
LSP-TUNNEL-REOPT:Tunnel1 [10002] set as reopt
LSP-TUNNEL-REOPT:Tunnel1 path option 2 [10002] installing as current
LSP-TUNNEL-REOPT:Tunnel1 [2] removed as current
LSP-TUNNEL-REOPT:Tunnel1 [2] set to delayed clean
LSP-TUNNEL-REOPT:Tunnel1 [10002] removed as reopt
LSP-TUNNEL-REOPT:Tunnel1 [10002] set to current
```

debug mpls traffic-eng tunnels signalling

To print information about traffic engineering tunnel signaling operations, use the **debug mpls traffic-eng tunnels signalling** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels signalling** [**detail**] [*aclnum*]

Syntax Description	detail	(Optional) Prints detailed debugging information.
	aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information about only those traffic engineering tunnel signaling operations that match the access list.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the aclnum option were added.

Examples

In the following example, detailed debugging information is printed about traffic engineering tunnel signaling operations that match access list number 101:

```
debug mpls traffic-eng tunnels signalling detail 101

LSP-TUNNEL-SIG:tunnel Tunnel1 [2]:RSVP head-end open
LSP-TUNNEL-SIG:tunnel Tunnel1 [2]:received Path NHOP CHANGE
LSP-TUNNEL-SIG:Tunnel1 [2]:first hop change:0.0.0.0 --> 10.1.0.10
LSP-TUNNEL-SIG:received ADD RESV request for tunnel 10.106.0.6 1 [2]
LSP-TUNNEL-SIG:tunnel 10.106.0.6 1 [2]:path next hop is 10.1.0.10 (Et4/0/1)
LSP-TUNNEL-SIG:Tunnel1 [2] notified of new label information
LSP-TUNNEL-SIG:sending ADD RESV reply for tunnel 10.106.0.6 1 [2]
```

debug mpls traffic-eng tunnels state

To print information about state maintenance for traffic engineering tunnels, use the **debug mpls traffic-eng tunnels state** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels state** [**detail**] [*aclnum*]

Syntax Description

detail	(Optional) Prints detailed debugging information.
aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information about state maintenance for traffic engineering tunnels that match the access list.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

In the following example, detailed debugging information is printed about state maintenance for traffic engineering tunnels that match access list number 99:

```
debug mpls traffic-eng tunnels state detail 99

LSP-TUNNEL:tunnel 10.106.0.6 1 [2]: "Connected" -> "Disconnected"
LSP-TUNNEL:Tunnel1 received event:LSP has gone down
LSP-TUNNEL:tunnel 10.106.0.6 1 [2]: "Disconnected" -> "Dead"
LSP-TUNNEL-SIG:Tunnel1:changing state from up to down
LSP-TUNNEL:tunnel 10.106.0.6 1 [2]: "Dead" -> "Connected"
```

debug mpls traffic-eng tunnels timers

To print information about traffic engineering tunnel timer management, use the **debug mpls traffic-eng tunnels timers** privileged EXEC command. To disable debugging output, use the **no** form of this command.

[**no**] **debug mpls traffic-eng tunnels timers** [**detail**] [*aclnum*]

Syntax Description

detail	(Optional) Prints detailed debugging information.
aclnum	(Optional) Uses the specified access list to filter the debugging information. Prints information about traffic engineering tunnel timer management that matches the access list.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.05(S)	This command was introduced.
12.1(3)T	The **detail** keyword and the *aclnum* option were added.

Examples

In the following example, detailed debugging information is printed about traffic engineering tunnel timer management:

```
debug mpls traffic-eng tunnels timers detail

LSP-TUNNEL-TIMER:timer fired for Action Scheduler
LSP-TUNNEL-TIMER:timer fired for Tunnel Head Checkup
```

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.

head-end—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.

tail-end—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.