



## Diff-Serv-aware Traffic Engineering (DS-TE)

---

This guide presents extensions made recently to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it Diff-Serv aware. Specifically, the bandwidth reservable on each link for constraint-based routing (CBR) purposes can now be managed through two bandwidth pools: a *global pool* and a *sub-pool*. The sub-pool can be limited to a smaller portion of the link bandwidth. Tunnels using the sub-pool bandwidth can then be used in conjunction with MPLS Quality of Service (QoS) mechanisms to deliver guaranteed bandwidth services end-to-end across the network.

The guide contains the following sections:

- Background and Overview, page 1
- Platforms and Interfaces Supported, page 3
- Prerequisites, page 4
- Configuration Tasks, page 4
- Configuration Examples, page 12
- Command Reference, page 21
- Debug Commands, page 102
- Glossary, page 104



**Note**

---

References made to specific page numbers are meant to help readers of the printed (Acrobat™ .PDF) form of this guide. On-line readers may simply click on the page number (or the underlined, colored, or bolded text) to go to the referenced page.

---

## Background and Overview

MPLS traffic engineering allows constraint-based routing of IP traffic. One of the constraints satisfied by CBR is the availability of required bandwidth over a selected path. Diff-Serv-aware Traffic Engineering extends MPLS traffic engineering to enable you to perform constraint-based routing of “guaranteed” traffic, which satisfies a more restrictive bandwidth constraint than that satisfied by CBR for regular traffic. The more restrictive bandwidth is termed a *sub-pool*, while the regular TE tunnel bandwidth is called the *global pool*. (The sub-pool is a portion of the global pool.) This ability to satisfy a more restrictive bandwidth constraint translates into an ability to achieve higher Quality of Service performance (in terms of delay, jitter, or loss) for the guaranteed traffic.

For example, DS-TE can be used to ensure that traffic is routed over the network so that, on every link, there is never more than 40 per cent (or any assigned percentage) of the link capacity of guaranteed traffic (for example, voice), while there can be up to 100 per cent of the link capacity of regular traffic. Assuming QoS mechanisms are also used on every link to queue guaranteed traffic separately from regular traffic, it then becomes possible to enforce separate “overbooking” ratios for guaranteed and regular traffic. (In fact, for the guaranteed traffic it becomes possible to enforce no overbooking at all—or even an underbooking—so that very high QoS can be achieved end-to-end for that traffic, even while for the regular traffic a significant overbooking continues to be enforced.)

Also, through the ability to enforce a maximum percentage of guaranteed traffic on any link, the network administrator can directly control the end-to-end QoS performance parameters without having to rely on over-engineering or on expected shortest path routing behavior. This is essential for transport of applications that have very high QoS requirements (such as real-time voice, virtual IP leased line, and bandwidth trading), where over-engineering cannot be assumed everywhere in the network.

DS-TE involves extending OSPF (Open Shortest Path First routing protocol), so that the available sub-pool bandwidth at each preemption level is advertised in addition to the available global pool bandwidth at each preemption level. And DS-TE modifies constraint-based routing to take this more complex advertised information into account during path computation.

## Benefits

Diff-Serv-aware Traffic Engineering enables service providers to perform separate admission control and separate route computation for discrete subsets of traffic (for example, voice and data traffic).

Therefore, by combining DS-TE with other IOS features such as QoS, the service provider can:

- Develop QoS services for end customers based on *signaled* rather than *provisioned* QoS
- Build the higher-revenue generating “strict-commitment” QoS services, without over-provisioning
- Offer virtual IP leased-line, Layer 2 service emulation, and point-to-point guaranteed bandwidth services including voice-trunking
- Enjoy the scalability properties offered by MPLS

## Related Features and Technologies

The DS-TE feature is related to OSPF, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

## Related Documents

For OSPF:

- “Configuring OSPF” in Cisco IOS Release 12.1 *IP and IP Routing Configuration Guide*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_c/ipcprt2/1cdospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_c/ipcprt2/1cdospf.htm)
- “OSPF Commands” in Cisco IOS Release 12.1 *IP and IP Routing Command Reference*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip\\_r/iprprt2/1rdospf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/ip_r/iprprt2/1rdospf.htm)

For RSVP:

- “Configuring RSVP” in Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_c/qcprt5/qcdrsvp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt5/qcdrsvp.htm)
- IP RSVP commands section in Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_r/qrdcmd2.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/qrdcmd2.htm)

For QoS:

- Cisco IOS Release 12.1 *Quality of Service Solutions Configuration Guide*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/index.htm)
- Cisco IOS Release 12.1 *Quality of Service Solutions Command Reference*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_r/index.htm)

For MPLS Traffic Engineering:

- Cisco IOS Release 12.1(3)T *MPLS Traffic Engineering and Enhancements*, <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/traffeng.htm>
- “Multiprotocol Label Switching” in Cisco IOS Release 12.1 *Switching Services Configuration Guide*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch\\_c/xcprt4](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_c/xcprt4)
- Section containing MPLS commands in Cisco IOS Release 12.1 *Switching Services Command Reference*, [http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch\\_r/xrdscmd3.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/switch_r/xrdscmd3.htm)

## Platforms and Interfaces Supported

This release supports DS-TE together with QoS on POS (Packet over Sonet) interfaces on the Cisco 12000 Series Gigabit Switch Router (GSR), with Engine 0 on edge (access) interfaces and Engine 2 on core (backbone) interfaces.

## Supported Standards

Standardization of Diff-Serv-aware MPLS Traffic Engineering is still in progress in the IETF (Internet Engineering Task Force). At the time of publication of this feature guide, DS-TE has been documented in the following IETF drafts:

- *Requirements for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham  
<http://search.ietf.org/internet-drafts/draft-ietf-mpls-diff-te-reqts-00.txt>
- *Extensions to RSVP-TE and CR-LDP for support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend, D. Skalecki & M. Tatham  
<http://search.ietf.org/internet-drafts/draft-ietf-mpls-diff-te-ext-00.txt>
- *Extensions to OSPF for Support of Diff-Serv-aware MPLS Traffic Engineering* by F. Le Faucheur, T. Nadeau, A. Chiu, W. Townsend & D. Skalecki  
<http://search.ietf.org/internet-drafts/draft-lefaucheur-diff-te-ospf-00.txt>

As the IETF work is still in progress, details are still under definition and subject to change, so DS-TE should be considered as a pre-standard implementation of IETF Diff-Serv-aware MPLS Traffic Engineering. However, it is in line with the requirements described in the first document above. The concept of "Class-Type" defined in that IETF draft corresponds to the concept of bandwidth pool implemented by DS-TE. And because DS-TE supports two bandwidth pools (global pool and sub-pool), DS-TE should be seen as supporting two Class-Types (Class-Type 0 and Class-Type 1).

## Prerequisites

Your network must support the following Cisco IOS features in order to support guaranteed bandwidth services based on Diff-Serv-aware Traffic Engineering:

- MPLS
- IP Cisco Express Forwarding (CEF)
- OSPF
- RSVP
- QoS

## Configuration Tasks

This section lists the minimum set of commands you need to implement the Diff-Serv-aware Traffic Engineering feature—in other words, to establish a tunnel that reserves bandwidth from the sub-pool.

The subsequent "Configuration Examples" section (page 10), presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

## New Commands

DS-TE commands were developed from the existing command set that configures MPLS traffic engineering. The only difference introduced to create DS-TE was the expansion of two commands:

- **ip rsvp bandwidth** was expanded to configure the size of the sub-pool on every link.
- **tunnel mpls traffic-eng bandwidth** was expanded to enable a TE tunnel to reserve bandwidth from the sub-pool.

### The ip rsvp bandwidth command

The old command was

```
ip rsvp bandwidth x y
```

where x = the size of the only possible pool, and y = the size of a single traffic flow (ignored by traffic engineering)

Now the extended command is

```
ip rsvp bandwidth x y sub-pool z
```

where x = the size of the global pool, and z = the size of the sub-pool.

(Remember, the sub-pool's bandwidth is less than—because it is part of—the global pool's bandwidth.)

## The tunnel mpls traffic-eng bandwidth command

The old command was

```
tunnel mpls traffic-eng bandwidth b
```

where b = the amount of bandwidth this tunnel requires.

Now you specify from which pool (global or sub) the tunnel's bandwidth is to come. You can enter

```
tunnel mpls traffic-eng bandwidth sub-pool b
```

This indicates that the tunnel should use bandwidth from the sub-pool. Alternatively, you can enter

```
tunnel mpls traffic-eng bandwidth b
```

This indicates that the tunnel should use bandwidth from the global pool (the default).

## The Configuration Procedure

To establish a sub-pool TE tunnel, you must enter configurations at three levels:

- the device (router or switch router)
- the physical interface
- the tunnel interface

On the first two levels, you activate traffic engineering; on the third level—the tunnel interface—you establish the sub-pool tunnel. Therefore, it is only at the tunnel headend device that you need to configure all three levels. At the tunnel midpoints and tail, it is sufficient to configure the first two levels.

In the tables below, each command is explained in brief. For a more complete explanation of any command, refer to the page given in the right-hand column.

### Level 1: Configuring the Device

At this level, you tell the device (switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding or CEF), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, and the Open Shortest Path First (OSPF) routing algorithm. This level is often called global configuration mode because the configuration is applied globally, to the entire device, rather than to a specific interface or routing instance. (These commands have not been modified from earlier releases of Cisco IOS.)

You enter the following commands:

	Command	Purpose
Step 1	Router(config)# <b>ip cef</b>	Enables CEF—which accelerates the flow of packets through the device. (More on page 30.)
Step 2	Router(config)# <b>mpls traffic-eng tunnels</b>	Enables MPLS, and specifically its traffic engineering tunnel capability. (More on page 44.)
Step 3	Router(config)# <b>router ospf</b>	Invokes the OSPF routing process for IP and puts the device into router configuration mode. (More on page 46.)

	Command	Purpose
Step 4	Router(config-router)# <b>mpls traffic-eng area num</b>	Turns on MPLS traffic engineering for a particular OSPF area. (More on page 35.)
Step 5	Router(config-router)# <b>mpls traffic-eng router-id loopback0</b>	Specifies that the traffic engineering router identifier is the IP address associated with the <i>loopback0</i> interface. (More on page 43.)

## Level 2: Configuring the Physical Interface

Having configured the device, you now must configure the interface on that device through which the tunnel will run. To do that, you first put the router into interface-configuration mode.

You then enable Resource Reservation Protocol. RSVP is used to signal (set up) a traffic engineering tunnel, and to tell devices along the tunnel path to reserve a specific amount of bandwidth for the traffic that will flow through that tunnel. It is with this command that you establish the maximum size of the sub-pool.

Finally, you enable the MPLS traffic engineering tunnel feature on this physical interface.

To accomplish these tasks, you enter the following commands:

	Command	Purpose
Step 1	Router(config)# <b>interface interface-id</b>	Moves configuration to the interface level, directing subsequent configuration commands to the specific interface identified by the <i>interface-id</i> . (More on page 26.)
Step 2	Router(config-if)# <b>ip rsvp bandwidth interface-kbps sub-pool kbps</b>	Enables RSVP on this interface and limits the amount of bandwidth RSVP can reserve on this interface. The sum of bandwidth used by all tunnels on this interface cannot exceed <i>interface-kbps</i> , and the sum of bandwidth used by all sub-pool tunnels cannot exceed <i>sub-pool kbps</i> . (More on page 32.)
Step 3	Router(config-if)# <b>mpls traffic-eng tunnels</b>	Enables the MPLS traffic engineering tunnel feature on this interface. (More on page 45.)

## Level 3: Configuring the Tunnel Interface

Now you create a set of attributes for the tunnel itself; those attributes are configured on the “tunnel interface” (not to be confused with the physical interface just configured above).

The only command which was modified at this level for DS-TE is **tunnel mpls traffic-eng bandwidth** (described in detail on page 96).

You enter the following commands:

	Command	Purpose
Step 1	Router(config)# <b>interface tunnel1</b>	Creates a tunnel interface (named in this example <b>tunnel1</b> ) and enters interface configuration mode. (More on page 26.)
Step 2	Router(config-if)# <b>tunnel destination A.B.C.D</b>	Specifies the IP address of the tunnel tail device. (More on page 90.)
Step 3	Router(config-if)# <b>tunnel mode mpls traffic-eng</b>	Sets the tunnel’s encapsulation mode to MPLS traffic engineering. (More on page 92.)

	Command	Purpose
Step 4	Router(config-if)# <b>tunnel mpls traffic-eng bandwidth {sub-pool   [global]} bandwidth</b>	Configures the tunnel's bandwidth and assigns it either to the sub-pool or the global pool. (More on page 96).
Step 5	Router(config-if)# <b>tunnel mpls traffic-eng priority</b>	Sets the priority to be used when system determines which existing tunnels are eligible to be preempted. (More on page 100).
Step 6	Router(config-if)# <b>tunnel mpls traffic-eng path-option</b>	Configures the paths (hops) a tunnel should use. The user can enter an explicit path (can specify the IP addresses of the hops) or can specify a dynamic path (the router figures out the best set of hops). (More on page 98).

## Verifying the Configurations

To view the complete configuration you have entered, use the EXEC command **show running-config** and check its output display for correctness.

To check *just one tunnel's* configuration, enter **show interfaces tunnel** followed by the tunnel interface number. And to see that tunnel's RSVP bandwidth and flow, enter **show ip rsvp interface** followed by the name or number of the physical interface.

Here is an example of the information displayed by these two commands. To see an explanation of each field used in the following displays turn to page 47 for **show interfaces tunnel** and page 61 for **show ip rsvp interface**.

```
GSR1#show interfaces tunnel 4
Tunnel4 is up, line protocol is down
Hardware is Routing Tunnel
MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
Tunnel source 0.0.0.0, destination 0.0.0.0
Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Output queue 0/0, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 0 bits/sec, 0 packets/sec
  0 packets input, 0 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets, 0 restarts

GSR1#show ip rsvp interface pos4/0
interface    allocated  i/f max  flow max sub max
PO4/0       300K      466500K 466500K  0M
```

To view *all tunnels at once* on the router you have configured, enter **show mpls traffic-eng tunnels brief**. The information displayed when tunnels are functioning properly looks like this (a table explaining the display fields begins on page 88):

```
GSR1#show mpls traffic-eng tunnels brief
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:            running
  Forwarding:              enabled
  Periodic reoptimization:  every 3600 seconds, next in 3029 seconds
TUNNEL NAME                DESTINATION      UP IF    DOWN IF  STATE/PROT
GSR1_t0                    192.168.1.13    -        SR3/0    up/up
GSR1_t1                    192.168.1.13    -        SR3/0    up/up
GSR1_t2                    192.168.1.13    -        PO4/0    up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

When one or more tunnels is not functioning properly, the display could instead look like this. (In the following example, tunnels t0 and t1 are down, as indicated in the far right column).

```
GSR1#show mpls traffic-eng tunnels brief
Signalling Summary:
  LSP Tunnels Process:      running
  RSVP Process:            running
  Forwarding:              enabled
  Periodic reoptimization:  every 3600 seconds, next in 2279 seconds
TUNNEL NAME                DESTINATION      UP IF    DOWN IF  STATE/PROT
GSR1_t0                    192.168.1.13    -        SR3/0    up/down
GSR1_t1                    192.168.1.13    -        SR3/0    up/down
GSR1_t2                    192.168.1.13    -        PO4/0    up/up
Displayed 3 (of 3) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

To find out *why* a tunnel is down, insert its name into this same command, after adding the keyword **name** and omitting the keyword **brief**. For example:

```
GSR1#show mpls traffic-eng tunnels name GSR1_t0
Name:GSR1_t0                      (Tunnel0) Destination:192.168.1.13
Status:
  Admin:up          Oper:down Path: not valid          Signalling:connected
```

If, as in this example, the Path is displayed as **not valid**, use the **show mpls traffic-eng topology** command to make sure the router has received the needed updates. (That command is described on page 85.)

Additionally, you can use any of the following **show** commands to inspect particular aspects of the network, router, or interface concerned:

To see information about...		Use this command
this level	and this item...	
Network	Advertised bandwidth allocation information	<b>show mpls traffic-eng link-management advertisements</b> (described on page 72)
	Preemptions along the tunnel path	<b>debug mpls traffic-eng link-management preemption</b> (described on 103)
	Available TE link bandwidth on all head routers	<b>show mpls traffic-eng topology</b> (described on page 85)

To see information about...		Use this command
this level	and this item...	
Router	Status of all tunnels currently signalled by this router	<b>show mpls traffic-eng link-management admission-control</b> (described on page 70)
	Tunnels configured on midpoint routers	<b>show mpls traffic-eng link-management summary</b> (described on page 83)
Physical interface	Detailed information on current bandwidth pools	<b>show mpls traffic-eng link-management bandwidth-allocation [interface-name]</b> (described on page 75)
	TE RSVP bookkeeping	<b>show mpls traffic-eng link-management interfaces</b> (described on page 81)
	Entire configuration of one interface	<b>show run interface</b>

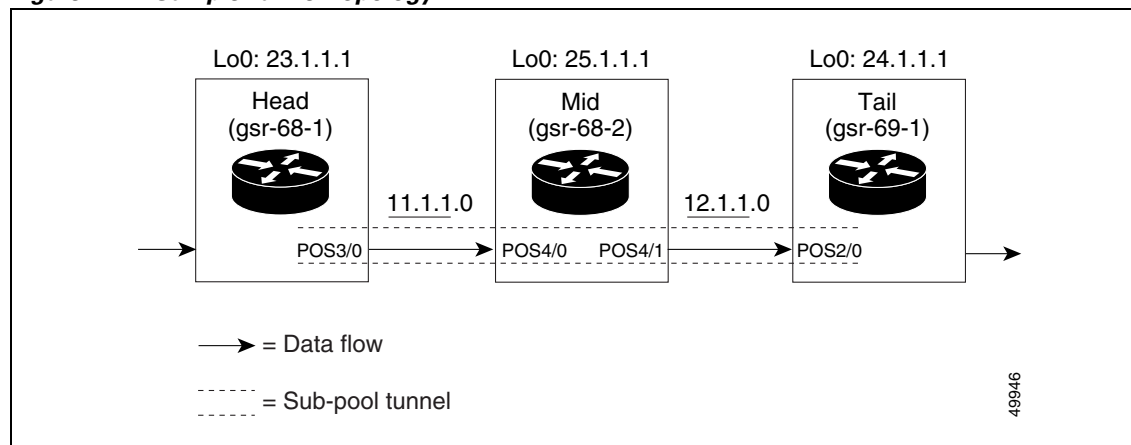
# Configuration Examples

This section first presents the DS-TE configuration needed to create the sub-pool tunnel. Then it presents the more comprehensive design for building end-to-end guaranteed bandwidth service, which involves configuring Quality of Service as well.

## DS-TE Configuration

As shown in Figure 1, the tunnel configuration involves at least three devices—tunnel head, midpoint, and tail. On each of those devices one or two physical interfaces must be configured, for traffic ingress and egress.

**Figure 1** Sample Tunnel Topology



## Tunnel Head

At the device level:

```
gsr-68-1# configure terminal
gsr-68-1(config)# ip cef
gsr-68-1(config)# mpls traffic-eng tunnels
gsr-68-1(config)# router ospf 100
  gsr-68-1(config-router)# redistribute connected
  gsr-68-1(config-router)# network 11.1.1.0 0.0.0.255 area 0
  gsr-68-1(config-router)# network 23.1.1.1 0.0.0.0 area 0
  gsr-68-1(config-router)# mpls traffic-eng router-id Loopback0
  gsr-68-1(config-router)# mpls traffic-eng area 0
  gsr-68-1(config-router)# exit
```

```
gsr-68-1(config)# interface Loopback0
```

At the physical interface level (internal):

```
gsr-68-1(config-if)# ip address 23.1.1.1 255.255.255.255
gsr-68-1(config-if)# no ip directed-broadcast
gsr-68-1(config-if)# exit
```

At the device level:

```
gsr-68-1(config)# interface POS3/0
```

49946

At the physical interface level (egress):

```
gsr-68-1(config-if)# ip address 11.1.1.1 255.255.255.0
gsr-68-1(config-if)# mpls traffic-eng tunnels
gsr-68-1(config-if)# ip rsvp bandwidth 500000 500000 sub-pool 300000
gsr-68-1(config-if)# exit
```

At the device level:

```
gsr-68-1(config)# interface Tunnel1
```

At the tunnel interface level:

```
gsr-68-1(config-if)# ip unnumbered Loopback0
gsr-68-1(config-if)# tunnel destination 24.1.1.1
gsr-68-1(config-if)# tunnel mode mpls traffic-eng
gsr-68-1(config-if)# tunnel mpls traffic-eng priority 0 0
gsr-68-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
gsr-68-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
gsr-68-1(config-if)# exit
gsr-68-1(config)#
```

## Midpoint Devices

At the device level:

```
gsr-68-2# configure terminal
gsr-68-2(config)# ip cef
gsr-68-2(config)# mpls traffic-eng tunnels

gsr-68-2(config)# router ospf 100
gsr-68-2(config-router)# network 10.1.1.0 0.0.0.255 area 0
gsr-68-2(config-router)# network 11.1.1.0 0.0.0.255 area 0
gsr-68-2(config-router)# network 12.1.1.0 0.0.0.255 area 0
gsr-68-2(config-router)# network 25.1.1.1 0.0.0.0 area 0
gsr-68-2(config-router)# mpls traffic-eng router-id Loopback0
gsr-68-2(config-router)# mpls traffic-eng area 0
gsr-68-2(config-router)# exit

gsr-68-2(config)# interface Loopback0
```

At the physical interface level (internal):

```
gsr-68-2(config-if)# ip address 25.1.1.1 255.255.255.255
gsr-68-2(config-if)# no ip directed-broadcast
gsr-68-2(config-if)# exit
```

At the device level:

```
gsr-68-2(config)# interface POS4/0
```

At the physical interface level (ingress):

```
gsr-68-2(config-if)# ip address 11.1.1.2 255.255.255.0
gsr-68-2(config-if)# mpls traffic-eng tunnels
gsr-68-2(config-if)# ip rsvp bandwidth 500000 500000 sub-pool 300000
gsr-68-2(config-if)# exit
```

At the device level:

```
gsr-68-2(config)# interface POS4/1
```

At the physical interface level (egress):

```
gsr-68-2(config-if)# ip address 12.1.1.2 255.255.255.0
gsr-68-2(config-if)# mpls traffic-eng tunnels
gsr-68-2(config-if)# ip rsvp bandwidth 500000 500000 sub-pool 300000
gsr-68-2(config-if)# exit
```

Note that there is no configuring of tunnel interfaces at the mid-point devices, only physical interfaces and the device globally.

## Tail-End Device

At the device level:

```
gsr-69-1# configure terminal
gsr-69-1(config)# ip cef
gsr-69-1(config)# mpls traffic-eng tunnels
gsr-69-1(config)# router ospf 100
gsr-69-1(config-router)# redistribute connected
gsr-69-1(config-router)# network 12.1.1.0 0.0.0.255 area 0
gsr-69-1(config-router)# network 24.1.1.1 0.0.0.0 area 0
gsr-69-1(config-router)# mpls traffic-eng router-id Loopback0
gsr-69-1(config-router)# mpls traffic-eng area 0
gsr-69-1(config-router)# exit
```

```
gsr-69-1(config)# interface Loopback0
```

At the physical interface level (internal):

```
gsr-69-1(config-if)# ip address 24.1.1.1 255.255.255.255
gsr-69-1(config-if)# no ip directed-broadcast
gsr-69-1(config-if)# exit
```

At the device level:

```
gsr-69-1(config)# interface POS2/0
```

At the physical interface level (ingress):

```
gsr-69-1(config-if)# ip address 12.1.1.3 255.255.255.0
gsr-69-1(config-if)# mpls traffic-eng tunnels
gsr-69-1(config-if)# exit
```

## Guaranteed Bandwidth Service Configuration

Having configured two bandwidth pools, you now can

- Use one pool, the sub-pool, for tunnels that carry traffic requiring strict bandwidth guarantees or delay guarantees
- Use the other pool, the global pool, for tunnels that carry traffic requiring only Differentiated Service.

Having a separate pool for traffic requiring strict guarantees allows you to limit the amount of such traffic admitted on any given link. Often, it is possible to achieve strict QoS guarantees only if the amount of guaranteed traffic is limited to a portion of the total link bandwidth.

Having a separate pool for other traffic (best-effort or diffserv traffic) allows you to have a separate limit for the amount of such traffic admitted on any given link. This is useful because it allows you to fill up links with best-effort/diffserv traffic, thereby achieving a greater utilization of those links.

### Providing Strict QoS Guarantees Using DS-TE Sub-pool Tunnels

A tunnel using sub-pool bandwidth can satisfy the stricter requirements if you do all of the following:

1. Select a queue—or in diffserv terminology, select a PHB (per-hop behavior)—to be used exclusively by the strict guarantee traffic. This shall be called the “GB queue.”

If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. On the Cisco Series 12000 that is the "low-latency" queue. You must configure the bandwidth of the queue to be at least equal to the bandwidth of the sub-pool.

If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used. On the Cisco 12000 you use one of the existing Modified Deficit Round Robin (MDRR) queues.

2. Ensure that the guaranteed traffic sent through the sub-pool tunnel is placed in the GB queue *at the outbound interface of every tunnel hop*, and that no other traffic is placed in this queue.

You do this by marking the traffic that enters the tunnel with a unique value in the mpls exp bits field, and steering only traffic with that marking into the GB queue.

3. Ensure that this GB queue is never oversubscribed; that is, see that no more traffic is sent into the sub-pool tunnel than the GB queue can handle.

You do this by rate-limiting the guaranteed traffic before it enters the sub-pool tunnel. The aggregate rate of all traffic entering the sub-pool tunnel should be less than or equal to the bandwidth capacity of the sub-pool tunnel. Excess traffic can be dropped (in the case of delay/jitter guarantees) or can be marked differently for preferential discard (in the case of bandwidth guarantees).

4. Ensure that the amount of traffic entering the GB queue is limited to an appropriate percentage of the total bandwidth of the corresponding outbound link. The exact percentage to use depends on several factors that can contribute to accumulated delay in your network: your QoS performance objective, the total number of tunnel hops, the amount of link fan-in along the tunnel path, burstiness of the input traffic, and so on.

You do this by setting the sub-pool bandwidth of each outbound link to the appropriate percentage of the total link bandwidth (that is, by adjusting the z parameter of the **ip rsvp bandwidth** command).

### Providing Differentiated Service Using DS-TE Global Pool Tunnels

You can configure a tunnel using global pool bandwidth to carry best-effort as well as several other classes of traffic. Traffic from each class can receive differentiated service if you do all of the following:

1. Select a separate queue (a distinct diffserv PHB) for each traffic class. For example, if there are three classes (gold, silver, and bronze) there must be three queues (diffserv AF2, AF3, and AF4).
2. Mark each class of traffic using a unique value in the MPLS experimental bits field (for example gold = 4, silver = 5, bronze = 6).
3. Ensure that packets marked as Gold are placed in the gold queue, Silver in the silver queue, and so on. The tunnel bandwidth is set based on the expected aggregate traffic across all classes of service.

To control the amount of diffserv tunnel traffic you intend to support on a given link, adjust the size of the global pool on that link.

### Providing Strict Guarantees and Differentiated Service in the Same Network

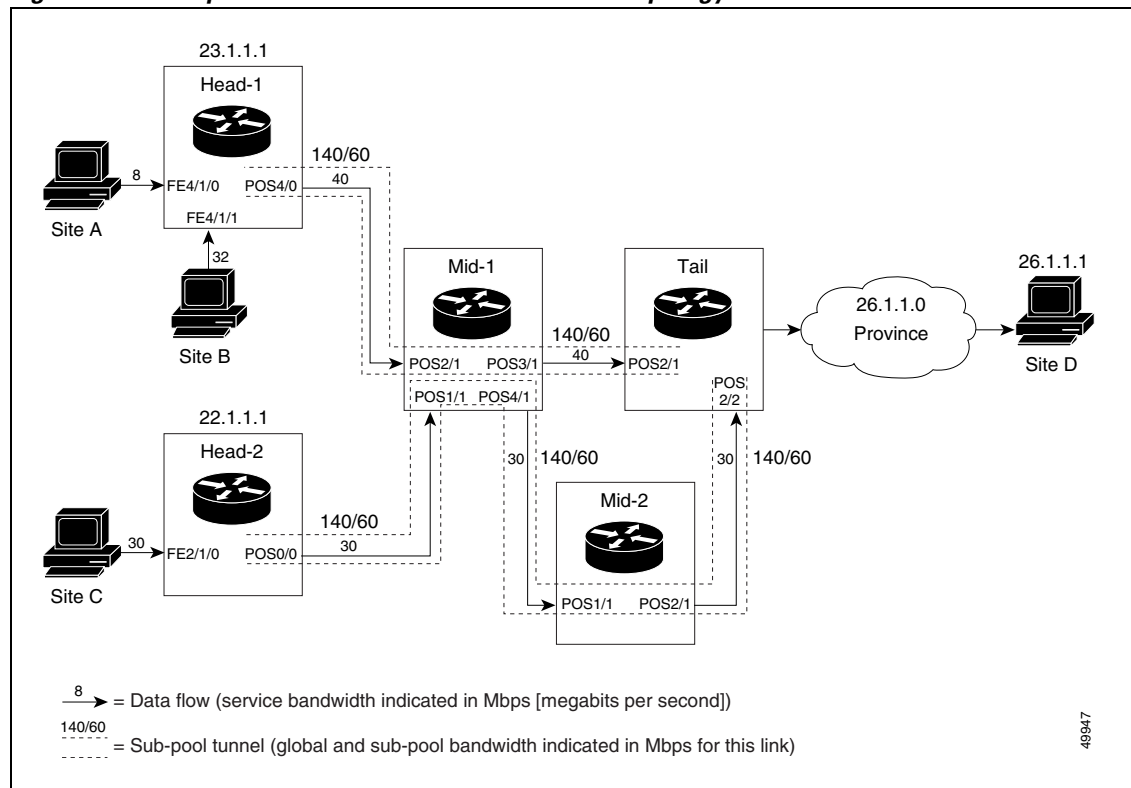
Because DS-TE allows simultaneous constraint-based routing of sub-pool and global pool tunnels, strict guarantees and diffserv can be supported simultaneously in a given network.

## Guaranteed Bandwidth Service Example

Figure 2 illustrates a topology for guaranteed bandwidth services whose destination is specified by a single prefix, either Site D (prefix 26.1.1.1) or subnet Province (prefix 26.1.1.0). Three services are offered:

- From Site A (defined as all traffic arriving at interface FE4/1/0): to host 26.1.1.1, 8 Mbps of guaranteed bandwidth with low loss, low delay and low jitter
- From Site B (defined as all traffic arriving at interface FE4/1/1): towards subnet 26.1.1.0, 32 Mbps of guaranteed bandwidth with low loss
- From Site C (defined as all traffic arriving at interface FE2/1/0): 30 Mbps of guaranteed bandwidth with low loss

**Figure 2** Sample Guaranteed Bandwidth Services Topology



These three services run through two sub-pool tunnels:

- From the router-1 head-1, 23.1.1.1, to the router-4 tail

- From the router-2 head-2, 22.1.1.1, to the router-4 tail

Thus both tunnels use the same tail router, though they have different heads. (In this picture the two tunnels also share one of the midpoint routers. In the real world there would of course be many more midpoints than just the two shown here.)

All POS interfaces in this example are OC3, whose capacity is 155 Mgps.

## Tunnel Head Configuration (Head-1)

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service on the subpool tunnel.

### Configuring the Pools and Tunnel

At the device level:

```
router-1(config)# ip cef
router-1(config)# mpls traffic-eng tunnels
router-1(config)# router ospf 100
router-1(config-router)# redistribute connected
router-1(config-router)# network 10.1.1.0 0.0.0.255 area 0
router-1(config-router)# network 23.1.1.1 0.0.0.0 area 0
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# mpls traffic-eng area 0
router-1(config-router)# exit
```

At the outgoing physical interface:

```
router-1(config)# interface pos4/0
router-1(config-if)# ip address 10.1.1.1 255.0.0.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-1(config-if)# exit
```

At the (internal) physical interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 23.1.1.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit
```

At the tunnel interface:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 27.1.1.1
router-1(config-if)# tunnel mode mpls traffic-eng
router-1(config-if)# tunnel mpls traffic-eng priority 0 0
router-1(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 40000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
```

To ensure that packets destined to host 26.1.1.1 and subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```
router-1(config)# ip route 26.1.1.0 255.255.255.0 Tunnel1
router-1(config)# exit
```

And in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-1(config)# no tunnel mpls traffic-eng autoroute announce
```

### For Service from Site A to Site D

At the inbound physical interface (FE4/1/0):

1. In global configuration mode, create an ACL 100 to refer to all packets destined to 26.1.1.1:

```
access-list 100 permit ip any host 26.1.1.1
```

2. Packets received on the inbound interface FE4/1/0 that match ACL 100 are rate-limited to:

- a. a rate of 8 Mgps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB
- d. Packets which conform to this rate are marked prec 5 and are forwarded
- e. Packets which exceed the rate are dropped

```
interface FastEthernet4/1/0
  rate-limit input access-group 100 8000000 1000000 2000000 conform-action \
  set-mpls-exp-transmit 5 exceed-action drop
```

3. Packets which do not match ACL 100 are rate-limited and, regardless of whether they conform or not, their precedence is set to zero and they are forwarded. Note that we do not really care to rate-limit these packets. The intention is simply to ensure that all these packets are marked with precedence zero. The values used for rate-limiting are irrelevant.

```
rate-limit input 2000000000 512000000 1024000000 conform-action \
  set-mpls-exp-transmit 0 exceed-action set-mpls-exp-transmit 0
```

### For Service from Site B to Subnet "Province"

At the inbound physical interface (FE4/1/1):

1. In global configuration mode, create an ACL 120 to refer to all packets destined to subnet 26.1.1.0:

```
access-list 120 permit ip any 26.1.1.0 255.255.255.255
```

2. Packets received on the inbound interface FE4/1/1 that match ACL 120 are rate-limited to:

- a. a rate of 32 Mgps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB
- d. Packets which conform to this rate are marked prec 5 and are forwarded
- e. Packets which exceed the rate are dropped

```
interface FastEthernet4/1/1
  rate-limit input access-group 120 32000000 1000000 2000000 conform-action \
  set-mpls-exp-transmit 5 exceed-action drop
```

3. Packets which do not match ACL 120 are rate-limited and, regardless of whether they conform or not, their precedence is set to zero and they are forwarded. Note that we do not really care to rate-limit these packets. The intention is simply to ensure that all these packets are marked with precedence zero. The values used for rate-limiting are irrelevant.

```
rate-limit input 2000000000 512000000 1024000000 conform-action \
set-mpls-exp-transmit 0 exceed-action set-mpls-exp-transmit 0
```

## For Both Services

The outbound interface (POS4/0) is configured as follows. At the device level, you create a profile of QoS queuing:

```
router-1(config)# cos-queue-group class0+5
router-1(config-cos-queue)# precedence 0 random-detect-label 0
router-1(config-cos-queue)# precedence 5 queue low-latency
router-1(config-cos-queue)# precedence 5 random-detect-label 5
router-1(config-cos-queue)# random-detect-label 0 100 200 1
router-1(config-cos-queue)# random-detect-label 5 2000 3000 1
router-1(config-cos-queue)# queue low-latency strict-priority
```

At the physical interface level:

```
router-1(config)# interface pos4/0
router-1(config-if)# tx-cos class0+5
```

As a result of all the above configuration lines, packets entering the Head-1 router via interface FE4/1/0 and destined for host 26.1.1.1, or entering that router via interface FE4/1/1 and destined for subnet 26.1.1.0, have their IP precedence field set to 5. It is assumed that no other packets entering this router (on any interface) are using this precedence. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another precedence value.) When exiting this router via interface POS4/0, packets marked with IP precedence 5 are placed in the low latency queue.



### Note

---

Packets entering the router via FE4/1/0 or FE4/1/1 and exiting POS4/0 enter as IP packets and exit as MPLS packets.

---

## Tunnel Head Configuration (Head-2)

First we recapitulate commands that establish two bandwidth pools and a sub-pool tunnel (as presented earlier in this Configuration Examples section). Then we present the QoS commands that guarantee end-to-end service.

## Configuring the Pools and Tunnel

At the device level:

```
router-2(config)# ip cef
router-2(config)# mpls traffic-eng tunnels
router-2(config)# router ospf 100
router-2(config-router)# redistribute connected
router-2(config-router)# network 11.1.1.0 0.0.0.255 area 0
router-2(config-router)# network 22.1.1.1 0.0.0.0 area 0
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# mpls traffic-eng area 0
router-2(config-router)# exit
```

At the outgoing physical interface:

```
router-2(config)# interface pos0/0
router-2(config-if)# ip address 11.1.1.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-2(config-if)# exit
```

At the (internal) physical interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 22.1.1.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit
```

At the tunnel interface:

```
router-2(config)# interface Tunnel2
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 27.1.1.1
router-2(config-if)# tunnel mode mpls traffic-eng
router-2(config-if)# tunnel mpls traffic-eng priority 0 0
router-2(config-if)# tunnel mpls traffic-eng bandwidth sub-pool 30000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-2(config-if)# exit
```

And to ensure that packets destined to subnet 26.1.1.0 are sent into the sub-pool tunnel, we create a static route, at the device level:

```
router-2(config)# ip route 26.1.1.0 255.255.255.0 Tunnel2
router-2(config)# exit
```

Finally, in order to make sure that the Interior Gateway Protocol (IGP) will not send any other traffic down this tunnel, we disable autoroute announce:

```
router-2(config)# no tunnel mpls traffic-eng autoroute announce
```

## For Service from Site C to Subnet "Province"

At the inbound physical interface (FE2/0):

1. In global configuration mode, create an ACL 130 to refer to all packets destined to 26.1.1.0:
 

```
access-list 130 permit ip any 26.1.1.0 255.255.255.255
```
2. Packets received on the inbound interface FE2/0 that match ACL 130 are rate-limited to:
  - a. a rate of 30 Mgps
  - b. a normal burst of 1 MB

- c. a maximum burst of 2 MB
- d. Packets which conform to this rate are marked prec 5 and are forwarded
- e. Packets which exceed the rate are dropped

```
interface FastEthernet2/0
  rate-limit input access-group 130 32000000 1000000 2000000 conform-action \
  set-mpls-exp-transmit 5 exceed-action drop
```

3. Packets which do not match ACL 130 are rate-limited and, regardless of whether they conform or not, their precedence is set to zero and they are forwarded. Note that we do not really care to rate-limit these packets. The intention is simply to ensure that all these packets are marked with precedence zero. The values used for rate-limiting are irrelevant.

```
rate-limit input 2000000000 512000000 1024000000 conform-action \
set-mpls-exp-transmit 0 exceed-action set-mpls-exp-transmit 0
```

For the outbound physical interface (POS0/0), you create, at the device level, a profile of QoS queuing:

```
router-1(config)# cos-queue-group class0+5
router-1(config-cos-queue)# precedence 0 random-detect-label 0
router-1(config-cos-queue)# precedence 5 queue low-latency
router-1(config-cos-queue)# precedence 5 random-detect-label 5
router-1(config-cos-queue)# random-detect-label 0 100 200 1
router-1(config-cos-queue)# random-detect-label 5 2000 3000 1
router-1(config-cos-queue)# queue low-latency strict-priority
```

And at the physical interface level:

```
router-1(config)# interface pos0/0
router-1(config-if)# tx-cos class0+5
```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1/0 and destined for subnet 26.1.1.0 have their IP precedence field set to 5. It is assumed that no other packets entering this router (on any interface) are using this precedence. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another precedence value.) When exiting this router via interface POS0/0, packets marked with IP precedence 5 are placed in the low latency queue.



**Note**

---

Packets entering the router via FE2/1/0 and exiting through POS0/0 enter as IP packets and exit as MPLS packets.

---

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnels

At the device level:

```
router-3(config)# ip cef
router-3(config)# mpls traffic-eng tunnels
router-3(config)# router ospf 100
router-3(config-router)# redistribute connected
router-3(config-router)# network 10.1.1.0 0.0.0.255 area 0
router-3(config-router)# network 11.1.1.0 0.0.0.255 area 0
router-3(config-router)# network 24.1.1.1 0.0.0.0 area 0
router-3(config-router)# network 12.1.1.0 0.0.0.255 area 0
router-3(config-router)# network 13.1.1.0 0.0.0.255 area 0
router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# mpls traffic-eng area 0
router-3(config-router)# exit
```

At the (internal) physical interface:

```
router-3(config)# interface Loopback0
router-3(config-if)# ip address 24.1.1.1 255.255.255.255
router-3(config-if)# no ip directed-broadcast
router-3(config-if)# exit
```

At the physical interface level (ingress):

```
router-3(config)# interface pos2/1
router-3(config-if)# ip address 10.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 11.1.1.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-3(config-if)# exit
```

At the physical interface level (egress):

```
router-3(config)# interface pos3/1
router-3(config-if)# ip address 12.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-3(config-if)# exit

router-3(config)# interface pos4/1
router-3(config-if)# ip address 13.1.1.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-3(config-if)# exit
```

## For All GB Services

At the device level, create a profile of QoS queuing:

```
router-3(config)# cos-queue-group class0+5
router-3(config-cos-queue)# precedence 0 random-detect-label 0
router-3(config-cos-queue)# precedence 5 queue low-latency
router-3(config-cos-queue)# precedence 5 random-detect-label 5
router-3(config-cos-queue)# random-detect-label 0 100 200 1
router-3(config-cos-queue)# random-detect-label 5 2000 3000 1
router-3(config-cos-queue)# queue low-latency strict-priority
```

## For Services from Sites A and B

At the physical interface level:

```
router-3(config)# interface pos3/1
router-3(config-if)# tx-cos class0+5
```

## For Service from Site C

At the physical interface level:

```
router-3(config)# interface pos4/1
router-3(config-if)# tx-cos class0+5
```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on the midpoint router are configured identically to the outbound interface of the head router (except, of course, for the IDs of the individual interfaces):

### Configuring the Pools and Tunnel

At the device level:

```
router-5(config)# ip cef
router-5(config)# mpls traffic-eng tunnels
router-5(config)# router ospf 100
router-5(config-router)# redistribute connected
router-5(config-router)# network 13.1.1.0 0.0.0.255 area 0
router-5(config-router)# network 14.1.1.0 0.0.0.255 area 0
router-5(config-router)# network 25.1.1.1 0.0.0.0 area 0
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# mpls traffic-eng area 0
router-5(config-router)# exit
```

At the (internal) physical interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 25.1.1.1 255.255.255.255
router-5(config-if)# no ip directed-broadcast
router-5(config-if)# exit
```

At the physical interface level (ingress):

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 13.1.1.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-5(config-if)# exit
```

At the physical interface level (egress):

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 14.1.1.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-5(config-if)# exit
```

## For Service from Site C

At the device level, create a profile of QoS queuing:

```
router-5(config)# cos-queue-group class0+5
router-5(config-cos-queue)# precedence 0 random-detect-label 0
router-5(config-cos-queue)# precedence 5 queue low-latency
router-5(config-cos-queue)# precedence 5 random-detect-label 5
router-5(config-cos-queue)# random-detect-label 0 100 200 1
router-5(config-cos-queue)# random-detect-label 5 2000 3000 1
router-5(config-cos-queue)# queue low-latency strict-priority
```

At the physical interface level:

```
router-5(config)# interface pos2/1
router-5(config-if)# tx-cos class0+5
```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured identically to the inbound interfaces of the midpoint router (except, of course, for the ID of each particular interface):

### Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef
router-4(config)# mpls traffic-eng tunnels
router-4(config)# router ospf 100
router-4(config-router)# redistribute connected
router-4(config-router)# network 12.1.1.0 0.0.0.255 area 0
router-4(config-router)# network 14.1.1.0 0.0.0.255 area 0
router-4(config-router)# network 27.1.1.1 0.0.0.0 area 0
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng area 0
router-4(config-router)# exit
```

At the (internal) physical interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 27.1.1.1 255.255.255.255
router-4(config-if)# no ip directed-broadcast
router-4(config-if)# exit
```

At the physical interface (ingress):

```
router-4(config)# interface pos2/1
router-4(config-if)# ip address 12.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 14.1.1.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
router-4(config-if)# exit
```

Because the tunnel ends on the tail (does not include any outbound interfaces of the tail router), no outbound QoS configuration is used.

# Command Reference

This section documents commands that configure guaranteed bandwidth services using Diff-Serv-aware Traffic Engineering tunnels. Besides the fundamental commands that were presented in the Configuration Tasks and Configuration Examples sections, we have included here advanced commands that enable you to fine-tune the behavior of traffic engineering tunnels.

- **interface**
- **ip cef**
- **ip rsvp bandwidth**
- **mpls traffic-eng administrative-weight**
- **mpls traffic-eng area**
- **mpls traffic-eng attribute-flags**
- **mpls traffic-eng backup-path tunnel**
- **mpls traffic-eng flooding thresholds**
- **mpls traffic-eng link timers bandwidth-hold**
- **mpls traffic-eng link timers periodic-flooding**
- **mpls traffic-eng reoptimize timers frequency**
- **mpls traffic-eng router-id**
- **mpls traffic-eng tunnels (configuration)**
- **mpls traffic-eng tunnels (interface)**
- **router ospf**
- **show interfaces tunnel**
- **show ip ospf**
- **show ip route**
- **show ip rsvp host**
- **show ip rsvp interface**
- **show mpls traffic-eng autoroute**
- **show mpls traffic-eng fast-reroute database**
- **show mpls traffic-eng fast-reroute log reroutes**
- **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 tunnels**
- **tunnel destination**
- **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 fast-reroute**
- **tunnel mpls traffic-eng path-option**
- **tunnel mpls traffic-eng priority**

# interface

Use the **interface** global configuration command to configure an interface type and enter interface configuration mode.

```
interface type number
```

## Cisco 7200 Series and Cisco 7500 Series with a Packet over SONET Interface Processor

```
interface type slot/port
```

## Cisco 7500 Series with Ports on VIP Cards

```
interface [type slot/port-adapter/port] [ethernet | serial]
```

## Cisco 7500 Series with Channelized T1 or E1

```
interface serial slot/port:channel-group
```

## Cisco 4000 Series with Channelized T1 or E1 and the Cisco MC3810

```
interface serial number:channel-group
```

## Cisco 7500 Series with Ports on VIP Cards (subinterface , global configuration)

```
interface type slot/port-adapter/port.subinterface-number { multipoint | point-to-point }
```

## Cisco 7200 Series (subinterface , global configuration)

```
interface type slot/port.subinterface-number { multipoint | point-to-point }
```

## Cisco 7500 Series (subinterface , global configuration)

```
interface type slot/port-adapter.subinterface-number { multipoint | point-to-point }
```

### Syntax Description

<i>type</i>	Type of interface to be configured. See Table 1.
<i>number</i>	Port, connector, or interface card number. On a Cisco 4000 series router, specifies the NPM number. The numbers are assigned at the factory at the time of installation or when added to a system, and can be displayed with the <b>show interfaces</b> command.
<i>slot</i>	Refer to the appropriate hardware manual for slot and port information.
<i>port</i>	Refer to the appropriate hardware manual for slot and port information.
<i>port-adapter</i>	Refer to the appropriate hardware manual for information about port adapter compatibility.

<i>:channel-group</i>	The Cisco 4000 series routers specifies the T1 channel group number in the range of 0 to 23 defined with the <b>channel-group</b> controller configuration command. On a dual port card, it is possible to run channelized on one port and primary rate on the other port.  The Cisco MC3810 specifies the T1/E1 channel group number in the range of 0 to 23 defined with the <b>channel-group</b> controller configuration command.
<i>.subinterface-number</i>	Subinterface number in the range 1 to 4294967293. The number that precedes the period (.) must match the number to which this subinterface belongs.
<b>multipoint   point-to-point</b>	(Optional) Specifies a multipoint or point-to-point subinterface. There is no default.

**Defaults**

No interface types are configured.

**Command Modes**

Global configuration

**Command History**

Release	Modification
10.0	This command was introduced for the Cisco 7000 series routers.
11.0	This command was introduced for the Cisco 4000 series routers.
11.2	This command was changed to change the <b>posi</b> keyword to <b>pos</b> .
11.3	This command was changed.
12.0	This command was changed to add the <b>switch</b> keyword.

**Usage Guidelines**

Subinterfaces can be configured to support partially meshed Frame Relay networks. Refer to the part entitled “Configuring Serial Interfaces” in the *Cisco IOS Interface Configuration Guide*.

There is no correlation between the number of the physical serial interface and the number of the logical LAN Extender interface. These interfaces can have the same or different numbers.

**Table 1** *interface Type Keywords*

Keyword	Interface Type
<b>async</b>	Port line used as an asynchronous interface.
<b>atm</b>	ATM interface.
<b>bri</b>	Integrated Services Digital Network (ISDN) Basic Rate Interface (BRI). This interface configuration is propagated to each of the B channels. B channels cannot be individually configured. The interface must be configured with dial-on-demand commands in order for calls to be placed on that interface.
<b>dialer</b>	Dialer interface.
<b>ethernet</b>	Ethernet IEEE 802.3 interface.

**Table 1** *interface Type Keywords (continued)*

<b>Keyword</b>	<b>Interface Type</b>
<b>fastethernet</b>	100-Mbps Ethernet interface on the Cisco 4500, Cisco 4700, Cisco 7000 and Cisco 7500 series routers.
<b>fddi</b>	Fiber Distributed Data Interface (FDDI).
<b>group-async</b>	Master asynchronous interface.
<b>hssi</b>	High-Speed Serial Interface (HSSI).
<b>lex</b>	LAN Extender (LEX) interface.
<b>loopback</b>	Software-only loopback interface that emulates an interface that is always up. It is a virtual interface supported on all platforms. The <i>interface-number</i> is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces you can create.
<b>null</b>	Null interface.
<b>port-channel</b>	Port channel interface
<b>pos</b>	Packet OC-3 interface on the Packet over SONET Interface Processor
<b>serial</b>	Serial interface.
<b>switch</b>	Switch interface
<b>tokenring</b>	Token Ring interface.
<b>tunnel</b>	Tunnel interface; a virtual interface. The <i>number</i> is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
<b>vg-anylan</b>	100VG-AnyLAN port adapter

**Examples**

The following example configures serial interface 0 with PPP encapsulation:

```
interface serial 0
 encapsulation ppp
```

The following example enables loopback mode and assigns an IP network address and network mask to the interface. The loopback interface established here will always appear to be up:

```
interface loopback 0
 ip address 131.108.1.1 255.255.255.0
```

The following example for the Cisco 7500 series router shows the interface configuration command for Ethernet port 4 on the EIP that is installed in (or recently removed from) slot 2:

```
interface ethernet 2/4
```

The following example begins configuration on the Token Ring interface processor in slot 1 on port 0 of a Cisco 7500 series routers:

```
interface tokenring 1/0
```

The following example shows how a partially meshed Frame Relay network can be configured. In this example, subinterface serial 0.1 is configured as a multipoint subinterface with three Frame Relay PVCs associated, and subinterface serial 0.2 is configured as a point-to-point subinterface.

```
interface serial 0
  encapsulation frame-relay
interface serial 0.1 multipoint
  ip address 131.108.10.1 255.255.255.0
  frame-relay interface-dlci 42 broadcast
  frame-relay interface-dlci 53 broadcast
interface serial 0.2 point-to-point
  ip address 131.108.11.1 255.255.0
  frame-relay interface-dlci 59 broadcast
```

The following example configures circuit 0 of a T1 link for Point-to-Point Protocol (PPP) encapsulation:

```
controller t1 4/1
circuit 0 1
interface serial 4/1:0
  ip address 131.108.13.1 255.255.255.0
  encapsulation ppp
```

The following example configures LAN Extender interface 0:

```
interface lex 0
```

#### Related Commands

Command	Description
<b>controller</b>	Configures a T1 or E1 controller and enters controller configuration mode.
<b>mac-address</b>	Sets the MAC layer address of the Cisco Token Ring.
<b>ppp</b>	Starts an asynchronous connection using PPP.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
<b>slip</b>	Starts a serial connection to a remote host using SLIP.

# ip cef

To enable Cisco Express Forwarding (CEF) on the route processor card, use the **ip cef** global configuration command. To disable CEF, use the **no** form of this command.

**ip cef [distributed]**

**no ip cef [distributed]**

## Syntax Description

<b>distributed</b>	(Optional) Enables distributed CEF (dCEF) operation. Distributes CEF information to line cards. Line cards perform express forwarding.
--------------------	--

## Defaults

On this platform...	The default is...
Cisco 7000 series equipped with RSP7000	CEF is not enabled.
Cisco 7200 series	CEF is not enabled.
Cisco 7500 series	CEF is enabled.
Cisco 12000 series Gigabit Switch Router	Distributed CEF is enabled.

## Command Modes

Global configuration

## Command History

Release	Modification
11.1 CC	This command was introduced.

## Usage Guidelines

This command is not available on the Cisco 12000 series GSR because that router series operates only in distributed CEF mode.

CEF is advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with dynamic, topologically dispersed traffic patterns, such as those associated with Web-based applications and interactive sessions.

## Examples

The following example enables standard CEF operation:

```
ip cef
```

The following example enables dCEF operation:

```
ip cef distributed
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>ip route-cache cef</b>	Reenables disabled CEF or DCEF operation on an interface.

## ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** interface configuration command. To disable RSVP completely, use the **no** form of this command. To eliminate only the sub-pool portion of the bandwidth, use the **no** form of this command with the keyword **sub-pool**.

**ip rsvp bandwidth** *interface-kbps single-flow-kbps* [**sub-pool kbps**]

**no ip rsvp bandwidth** *interface-kbps single-flow-kbps* [**sub-pool kbps**]

### Syntax Description

<i>interface-kbps</i>	Amount of bandwidth (in kbps) on interface to be reserved. The range is 1 to 10000000.
<i>single-flow-kbps</i>	Amount of bandwidth (in kbps) allocated to a single flow. [Ignored in DS-TE]. The range is 1 to 10000000.
<b>sub-pool kbps</b>	Amount of bandwidth (in kbps) on interface to be reserved to a portion of the total. The range is from 1 to the value of <i>interface-kbps</i> .

### Defaults

RSVP is disabled if this command is not entered. When enabled without the optional arguments, RSVP is enabled and 75 percent of the link bandwidth is reserved for it.

### Command Modes

Interface configuration

### Command History

Release	Modification
11.2	This command was introduced.
12.0(11)ST	Sub-pool option was added.

### Usage Guidelines

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).  
 RSVP is disabled by default to allow backward compatibility with systems that do not implement RSVP.  
 Weighted Random Early Detection (WRED) or fair queuing must be enabled first.

Related Commands	Command	Description
	<b>fair-queue (WFQ)</b>	Enables WFQ for an interface.
	<b>ip rsvp neighbor</b>	Enables neighbors to request a reservation.
	<b>ip rsvp reservation</b>	Enables a router to behave like it is receiving and forwarding RSVP RESV messages.
	<b>ip rsvp sender</b>	Enables a router to behave like it is receiving and forwarding RSVP PATH messages.
	<b>ip rsvp udp-multicasts</b>	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
	<b>random-detect (interface)</b>	Enables WRED or DWRED.
	<b>show ip rsvp installed</b>	Displays RSVP-related installed filters and corresponding bandwidth information.
	<b>show ip rsvp interface</b>	Displays RSVP-related interface information.
	<b>show ip rsvp neighbor</b>	Displays current RSVP neighbors.
	<b>show ip rsvp reservation</b>	Displays RSVP-related receiver information currently in the database.
	<b>show ip rsvp sender</b>	Displays RSVP PATH-related sender information currently in the database.

# mpls traffic-eng administrative-weight

To override the Interior Gateway Protocol's (IGPs) 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**

<b>Syntax Description</b>	<i>weight</i>	Cost of the link.
<b>Defaults</b>	IGP cost of the link.	
<b>Command Modes</b>	Interface configuration	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
<b>Examples</b>	<p>The following example overrides the IGP's cost of the link and sets the cost to 20:</p> <pre>Router(config-if)# mpls traffic-eng administrative-weight 20</pre>	
<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mpls traffic-eng attribute-flags</b>	Sets the user-specified attribute flags for an interface.

# mpls traffic-eng area

To configure a router running 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*

<b>Syntax Description</b>	<i>num</i>	The OSPF area on which MPLS traffic engineering is enabled.								
<b>Defaults</b>	No default behavior or values.									
<b>Command Modes</b>	Router configuration									
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(5)S</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.0(5)S	This command was introduced.					
Release	Modification									
12.0(5)S	This command was introduced.									
<b>Usage Guidelines</b>	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.									
<b>Examples</b>	<p>The following example configures a router running OSPF MPLS to flood traffic engineering for OSPF 0:</p> <pre>Router(config-router)# mpls traffic-eng area 0</pre>									
<b>Related Commands</b>	<table border="1"> <thead> <tr> <th>Command</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>mpls traffic-eng router-id</b></td> <td>Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.</td> </tr> <tr> <td><b>network area</b></td> <td>Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.</td> </tr> <tr> <td><b>router ospf</b></td> <td>Configures an OSPF routing process on a router.</td> </tr> </tbody> </table>	Command	Description	<b>mpls traffic-eng router-id</b>	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.	<b>network area</b>	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.	<b>router ospf</b>	Configures an OSPF routing process on a router.	
Command	Description									
<b>mpls traffic-eng router-id</b>	Specifies that the traffic engineering router identifier for the node is the IP address associated with a given interface.									
<b>network area</b>	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.									
<b>router ospf</b>	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

<i>attributes</i>	Links attributes to be compared with a tunnel's affinity bits during path selection. Range is 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

The following example sets the attribute flags to 0x0101:

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

## Related Commands

Command	Description
<b>mpls traffic-eng administrative weight</b>	Overrides the Interior Gateway Protocol's (IGPs) administrative weight of the link.
<b>tunnel mpls traffic-eng affinity</b>	Configures affinity (the properties the tunnel requires in its links) for an MPLS traffic engineering tunnel.

# mpls traffic-eng backup-path tunnel

To configure the interface to use a backup tunnel in the event of a detected failure on the interface, use the **mpls traffic-eng backup tunnel** interface command.

**mpls traffic-eng backup-path tunnel** *interface*

<b>Syntax Description</b>	<i>interface</i>	IP address associated with the given interface.
---------------------------	------------------	---

**Defaults** No default behavior or values.

**Command Modes** Interface

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(8)ST	This command was introduced.

**Examples** The following example shows you how to specify the traffic engineering backup tunnel with the ID of 1000:

```
Router(config_if)# mpls traffic-eng backup-path Tunnel1000
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show tunnel mpls traffic-eng fast-reroute</b>	Displays information about fast reroute for MPLS traffic engineering
	<b>tunnel mpls traffic-eng fast-reroute</b>	Enables an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure (assuming a backup tunnel exists).

# 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

<b>down</b>	Sets the thresholds for decreased resource availability.
<b>up</b>	Sets the thresholds for increased resource availability.
<i>percent</i> [ <i>percent</i> ]	Specifies the bandwidth threshold level. For <b>down</b> , you can enter a number from 0 through 99. For <b>up</b> , you can enter a number from 1 through 100.

## Defaults

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 may be flooded periodically unless periodic flooding was disabled.

## Examples

The following example sets the link's reserved bandwidth 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
<b>mpls traffic-eng link-management timers periodic-flooding</b>	Sets the length of the interval used for periodic flooding.

<b>Command</b>	<b>Description</b>
<b>show mpls traffic-eng link-management advertisements</b>	Shows local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
<b>show mpls traffic-eng link-management bandwidth-allocation</b>	Shows current local link information.

# mpls traffic-eng link timers bandwidth-hold

To set the length of time that bandwidth is "held" for an RSVP PATH (Set Up) message while waiting for the corresponding RSVP RESV message to come back, use the **mpls traffic-eng link timers bandwidth-hold** command

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

## Syntax Description

hold-time	Sets the length of time that bandwidth can be held. The range is from 1 to 300 seconds.
-----------	---

## Defaults

15 seconds

## Command Modes

Configuration

## Command History

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

## Examples

The following example sets the length of time that bandwidth is held to 10 seconds.

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

Table 16 lists the fields displayed in this example.

## Related Commands

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

# mpls traffic-eng link timers periodic-flooding

To set the length of the interval used for periodic flooding, use the **mpls traffic-eng link timers periodic-flooding** command.

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

## Syntax Description

interval	Length of interval used for periodic flooding (in seconds). The range is 0-3600. If you set this value to 0, you turn off periodic flooding. If you set this value anywhere in the range from 1 to 29, it is treated as 30.
----------	---

## Defaults

3 minutes

## Command Modes

Configuration

## Command History

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

## Usage Guidelines

Use this command to set the length of the interval used for periodic flooding to advertise link state information changes that do not trigger immediate action (for example, a change to the amount of bandwidth allocated that does not cross a threshold).

## Examples

The following example sets the interval length for periodic flooding to advertise flooding changes to 120 seconds.

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

## Related Commands

Command	Description
<b>mpls traffic-eng flooding thresholds</b>	Sets a link's reserved bandwidth threshold.

# mpls traffic-eng reoptimize timers frequency

To control the frequency at which tunnels with established LSPs are checked for better LSPs, use the **mpls traffic-eng reoptimize timers frequency** command.

**mpls traffic-eng reoptimize timers frequency** *seconds*

## 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 and, if successful, replaces the old and inferior LSP with the new and better LSP.

## Examples

The following example sets the reoptimization frequency to one day.

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

## Related Commands

Command	Description
<b>mpls traffic-eng reoptimize (exec)</b>	Does a reoptimization check now.
<b>tunnel mpls traffic-eng lockdown</b>	Does not do a reoptimization check on this tunnel.

# 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	<i>interface-name</i>	Interface whose primary IP address should be used for the router 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 identifier acts as a stable IP address for the traffic engineering configuration. This stable IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, the tunnel destination must be set to the destination node's traffic engineering router identifier, since that is the address the traffic engineering topology database at the tunnel head uses for its path calculation.
------------------	---

Examples	The following example specifies that the traffic engineering router identifier is the IP address associated with interface Loopback0:
----------	---

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

Related Commands	Command	Description
	<b>mpls traffic-eng</b>	Turns on flooding of MPLS traffic engineering link information into the indicated IGP level/area.

# mpls traffic-eng tunnels

## (global configuration mode)

To enable MPLS traffic engineering tunnel signalling 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. To use the feature, MPLS traffic engineering must also be enabled on the desired interfaces.

---

**Examples** The following example turns on the MPLS traffic engineering feature for a device:

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

---

Related Commands	Command	Description
	<b>mpls traffic-eng tunnels</b> (interface)	Enables MPLS traffic engineering tunnel signalling on an interface.

---

# mpls traffic-eng tunnels

## (interface configuration mode)

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

**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** This command enables 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 signalling requests.

---

**Examples** The following example turns on MPLS traffic engineering on interface Ethernet0/0:

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

---

Related Commands	Command	Description
	<b>mpls traffic-eng tunnels</b> (configuration)	Enables MPLS traffic engineering tunnel signalling on a device.

---

# router ospf

To configure an OSPF routing process, use the **router ospf** global configuration command. To terminate an OSPF routing process, use the **no** form of this command.

**router ospf** *process-id*

**no router ospf** *process-id*

<b>Syntax Description</b>	<i>process-id</i>	Internally used identification parameter for an OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each OSPF routing process.
---------------------------	-------------------	---

<b>Defaults</b>	No OSPF routing process is defined.
-----------------	-------------------------------------

<b>Command Modes</b>	Global configuration
----------------------	----------------------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

<b>Usage Guidelines</b>	You can specify multiple OSPF routing processes in each router.
-------------------------	---

<b>Examples</b>	The following example configures an OSPF routing process and assign a process number of 109: <pre>router ospf 109</pre>
-----------------	--

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>network area</b>	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

# show interfaces tunnel

To list tunnel interface information, use the **show interfaces tunnel** privileged EXEC command.

**show interfaces tunnel** *number* [**accounting**]

Syntax Description	
<i>number</i>	Port line number.
<b>accounting</b>	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	10.0	This command was introduced.

## Examples

The following is sample output from the **show interfaces tunnel** command:

```
Router# show interfaces tunnel 4

Tunnel4 is up, line protocol is down
  Hardware is Routing Tunnel
  MTU 1500 bytes, BW 9 Kbit, DLY 500000 usec, rely 255/255, load 1/255
  Encapsulation TUNNEL, loopback not set, keepalive set (10 sec)
  Tunnel source 0.0.0.0, destination 0.0.0.0
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  Five minute input rate 0 bits/sec, 0 packets/sec
  Five minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets, 0 restarts
```

Table 2 describes significant fields shown in the display.

**Table 2** *show interfaces tunnel Field Descriptions*

Field	Description
Tunnel is {up   down}	Interface is currently active and inserted into ring (up) or inactive and not inserted (down).  On the Cisco 7500 series routers, this displays the interface processor type, slot number, and port number.
line protocol is {up   down   administratively down}	Shows line protocol up if a valid route is available to the tunnel destination. Shows line protocol down if no route is available, or if the route would be recursive.

Table 2 show interfaces tunnel Field Descriptions (continued)

Field	Description
Hardware	Specifies the hardware type.
MTU	Maximum Transmission Unit of the interface.
BW	Bandwidth of the interface in kilobits per second.
DLY	Delay of the interface in microseconds.
rely	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability), calculated as an exponential average over 5 minutes.
load	Load on the interface as a fraction of 255 (255/255 is completely saturated), calculated as an exponential average over 5 minutes.
Encapsulation	Encapsulation method is always TUNNEL for tunnels.
loopback	Indicates whether loopback is set or not.
keepalive	Indicates whether keepalives are set or not.
Tunnel source	IP address used as the source address for packets in the tunnel.
destination	IP address of the host destination.
Tunnel protocol	Tunnel transport protocol (the protocol the tunnel is using). This is based on the <b>tunnel mode</b> command, which defaults to GRE.
key	ID key for the tunnel interface, unless disabled.
sequencing	Indicates whether the tunnel interface drops datagrams that arrive out of order. Can be disabled.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface.
output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the "last" fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks are printed.
Last clearing	Time at which the counters that measure cumulative statistics (such as number of bytes transmitted and received) shown in this report were last reset to zero. Note that variables that might affect routing (for example, load and reliability) are not cleared when the counters are cleared.  *** indicates the elapsed time is too large to be displayed. 0:00:00 indicates the counters were cleared more than $2^{31}$ ms (and less than $2^{32}$ ms) ago.
Output queue, drops Input queue, drops	Number of packets in output and input queues. Each number is followed by a slash, the maximum size of the queue, and the number of packets dropped due to a full queue.

**Table 2** *show interfaces tunnel Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
Five minute input rate, Five minute output rate	Average number of bits and packets transmitted per second in the last 5 minutes.  The 5-minute input and output rates should be used only as an approximation of traffic per second during a given 5-minute period. These rates are exponentially weighted averages with a time constant of 5 minutes. A period of four time constants must pass before the average will be within two percent of the instantaneous rate of a uniform stream of traffic over that period.
packets input	Total number of error-free packets received by the system.
bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
no buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernet networks and bursts of noise on serial lines are often responsible for no input buffer events.
broadcasts	Total number of broadcast or multicast packets received by the interface.
runts	Number of packets that are discarded because they are smaller than the medium's minimum packet size.
giants	Number of packets that are discarded because they exceed the medium's maximum packet size.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far-end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of a station transmitting bad data.
frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets.
overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the receiver's ability to handle the data.
ignored	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different than the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be increased.
abort	Illegal sequence of one bits on a serial interface. This usually indicates a clocking problem between the serial interface and the data link equipment.
packets output	Total number of messages transmitted by the system.
bytes	Total number of bytes, including data and MAC encapsulation, transmitted by the system.

**Table 2** *show interfaces tunnel Field Descriptions (continued)*

<b>Field</b>	<b>Description</b>
underruns	Number of times that the far-end transmitter has been running faster than the near-end router's receiver can handle. This may never be reported on some interfaces.
output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this may not balance with the sum of the enumerated output errors, as some datagrams may have more than one error, and others may have errors that do not fall into any of the specifically tabulated categories.
collisions	Number of messages retransmitted due to an Ethernet collision. This usually is the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). Some collisions are normal. However, if your collision rate climbs to around 4 or 5%, you should consider verifying that there is no faulty equipment on the segment and/or moving some existing stations to a new segment. A packet that collides is counted only once in output packets.
interface resets	Number of times an interface has been reset. The interface may be reset by the administrator or automatically when an internal error occurs.
restarts	Number of times the controller was restarted because of errors.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
<b>show ip route</b>	Displays the current state of the routing table.

# show ip ospf

To display general information about OSPF routing processes, use the **show ip ospf** EXEC command.

**show ip ospf** [*process-id*]

<b>Syntax Description</b>	<i>process-id</i>	(Optional) Process ID. If this argument is included, only information for the specified routing process is included.
---------------------------	-------------------	--

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	10.0	This command was introduced.

**Examples** The following is sample output from the **show ip ospf** command when entered without a specific OSPF process ID:

```
Router# show ip ospf

Routing Process "ospf 201" with ID 192.42.110.200
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
  igrp 200 with metric mapped to 2, includes subnets in redistribution
  rip with metric mapped to 2
  igrp 2 with metric mapped to 100
  igrp 32 with metric mapped to 1
Number of areas in this router is 3
Area 192.42.110.0
  Number of interfaces in this area is 1
  Area has simple password authentication
  SPF algorithm executed 6 times
```

Table 3 describes significant fields shown in the display.

**Table 3** show ip ospf Field Descriptions

Field	Description
Routing process "ospf 201" with ID 192.42.110.200	Process ID and OSPF router ID.
Supports ...	Number of Types of service supported (Type 0 only).
It is ...	Possible types are internal, area border, or autonomous system boundary.
Summary Link update interval	Specify summary update interval in hours:minutes:seconds, and time to next update.
External Link update interval	Specify external update interval in hours:minutes:seconds, and time to next update.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Number of areas	Number of areas in router, area addresses, and so on.
Link State Update Interval	Specify router and network link state update interval in hours:minutes:seconds, and time to next update.
Link State Age Interval	Specify max-aged update deletion interval and time until next database cleanup in hours:minutes:seconds.

The following is sample output from the **show ip ospf** command when entered on a router configured for Diff-Serv-aware Traffic Engineering:

```
router-2# show ip ospf
Routing Process "ospf 100" with ID 24.1.1.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x0
Number of opaque AS LSA 0. Checksum Sum 0x0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0) (Inactive)
    Number of interfaces in this area is 2
    Area has RRR enabled
    Area has no authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x14D81
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

# show ip route

Use the **show ip route** EXEC command to display the current state of the routing table.

```
show ip route [address [mask] [longer-prefixes]] | [protocol [process-id]]
```

Syntax Description		
<i>address</i>	(Optional) Address about which routing information should be displayed.	
<i>mask</i>	(Optional) Argument for a subnet mask.	
<b>longer-prefixes</b>	(Optional) The <i>address</i> and <i>mask</i> pair becomes a prefix and any routes that match that prefix are displayed.	
<i>protocol</i>	(Optional) Name of a routing protocol; or the keyword <b>connected</b> , <b>static</b> , or <b>summary</b> . If you specify a routing protocol, use one of the following keywords: <b>bgp</b> , <b>egp</b> , <b>eigrp</b> , <b>hello</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , or <b>rip</b> .	
<i>process-id</i>	(Optional) Number used to identify a process of the specified protocol.	

Command Modes	
EXEC	

## Examples

Command History	Release	Modification
	10.0	This command was introduced.
	10.3	The <i>process-id</i> argument was added.
	11.0	The <b>longer-prefixes</b> keyword was added.
	11.3	The output of the <b>show ip route</b> <i>IP-address</i> command was enhanced to display the origination of an IP route in IS-IS networks.

**Examples**

The following is sample output from the **show ip route** command when entered without an address:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
       C - connected, S - static, E - EGP derived, B - BGP derived
       * - candidate default route, IA - OSPF inter area route
       E1 - OSPF external type 1 route, E2 - OSPF external type 2 route

Gateway of last resort is 131.119.254.240 to network 129.140.0.0

O E2 150.150.0.0 [160/5] via 131.119.254.6, 0:01:00, Ethernet2
E    192.67.131.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
O E2 192.68.132.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
O E2 130.130.0.0 [160/5] via 131.119.254.6, 0:00:59, Ethernet2
E    128.128.0.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E    129.129.0.0 [200/129] via 131.119.254.240, 0:02:22, Ethernet2
E    192.65.129.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E    131.131.0.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E    192.75.139.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E    192.16.208.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E    192.84.148.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E    192.31.223.0 [200/128] via 131.119.254.244, 0:02:22, Ethernet2
E    192.44.236.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
E    140.141.0.0 [200/129] via 131.119.254.240, 0:02:22, Ethernet2
E    141.140.0.0 [200/129] via 131.119.254.240, 0:02:23, Ethernet2
```

The following is sample output that includes some IS-IS Level 2 routes learned:

```
Router# show ip route

Codes: I - IGRP derived, R - RIP derived, O - OSPF derived
       C - connected, S - static, E - EGP derived, B - BGP derived
       i - IS-IS derived
       * - candidate default route, IA - OSPF inter area route
E1 - OSPF external type 1 route, E2 - OSPF external type 2 route
L1 - IS-IS level-1 route, L2 - IS-IS level-2 route

Gateway of last resort is not set

160.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C    160.89.64.0 255.255.255.0 is possibly down,
     routing via 0.0.0.0, Ethernet0
i L2 160.89.67.0 [115/20] via 160.89.64.240, 0:00:12, Ethernet0
i L2 160.89.66.0 [115/20] via 160.89.64.240, 0:00:12, Ethernet0
```

Table 4 describes significant fields shown in these two displays.

**Table 4** *show ip route Field Descriptions*

Field	Description
O	Indicates protocol that derived the route. Possible values include the following: <ul style="list-style-type: none"> <li>• I—IGRP derived</li> <li>• R—RIP derived</li> <li>• O—OSPF derived</li> <li>• C—connected</li> <li>• S—static</li> <li>• E—EGP derived</li> <li>• B—BGP derived</li> <li>• i—IS-IS derived</li> </ul>
E2	Type of route. Possible values include the following: <ul style="list-style-type: none"> <li>• *—Indicates the last path used when a packet was forwarded. It pertains only to the non-fast-switched packets. However, it does not indicate what path will be used next when forwarding a non-fast-switched packet, except when the paths are equal cost.</li> <li>• IA—OSPF interarea route.</li> <li>• E1—OSPF external type 1 route.</li> <li>• E2—OSPF external type 2 route.</li> <li>• L1—IS-IS Level 1 route.</li> <li>• L2—IS-IS Level 2 route.</li> </ul>
150.150.0.0	Indicates the address of the remote network.
[160/5]	The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
via 131.119.254.6	Specifies the address of the next router to the remote network.
0:01:00	Specifies the last time the route was updated in hours:minutes:seconds.
Ethernet2	Specifies the interface through which the specified network can be reached.

When you specify that you want information about a specific network displayed, more detailed statistics are shown. The following is sample output from the **show ip route** command when entered with the address 131.119.0.0.

```
Router# show ip route 131.119.0.0

Routing entry for 131.119.0.0 (mask 255.255.0.0)
  Known via "igrp 109", distance 100, metric 10989
  Tag 0
  Redistributing via igrp 109
  Last update from 131.108.35.13 on TokenRing0, 0:00:58 ago
  Routing Descriptor Blocks:
  * 131.108.35.13, from 131.108.35.13, 0:00:58 ago, via TokenRing0
    Route metric is 10989, traffic share count is 1
    Total delay is 45130 microseconds, minimum bandwidth is 1544 Kbit
    Reliability 255/255, minimum MTU 1500 bytes
    Loading 2/255, Hops 4
```

When an IS-IS router advertises its link state information, it includes one of its own IP addresses to be used as the originator IP address. When other routers calculate IP routes, they can store the originator IP address with each route in the routing table.

The following example shows the output from the **show ip route** command when looking at an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next hop address, the second is the originator IP address from the advertising IS-IS router. This address helps you determine where a particular IP route has originated in your network. In the example the route to 10.0.0.1/32 was originated by a router with IP address 223.191.255.247.

```
Router# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 223.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
  * 10.22.22.2, from 223.191.255.247, via Serial2/3
    Route metric is 20, traffic share count is 1
    223.191.255.251, from 223.191.255.247, via Fddi1/0
    Route metric is 20, traffic share count is 1
```

Compare the report above using the **show ip route** command with an IP address to the following report using the **show ip route isis** command:

```
Router# show ip route isis

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
  i L1   10.0.0.1/32 [115/20] via 10.22.22.2, Serial2/3
         [115/20] via 223.191.255.251, Fddi1/0
  22.0.0.0/24 is subnetted, 2 subnets
  i L1   22.22.23.0 [115/20] via 223.191.255.252, Fddi1/0
```

Table 4 describes significant fields shown in this last display. Table 5 describes significant fields shown when using the **show ip route** command with an IP address (previous displays).

**Table 5** *show ip route with Address Field Descriptions*

Field	Description
Routing entry for 131.119.0.0 (mask 255.255.0.0)	Network number and mask.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
Tag	Integer that is used to implement the route.
Redistributing via ...	Indicates redistribution protocol.
Last update from 131.108.35.13 on ...	Indicates the IP address of a router that is the next hop to the remote network and the router interface on which the last update arrived.
0:00:58 ago	Specifies the last time the route was updated in hours:minutes:seconds.
131.108.35.13, from 131.108.35.13, 0:00:58 ago	Indicates the next hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received in hours:minutes:seconds.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
from...via ...	The first address is the next hop IP address, and the other is the information source. This report is followed by the interface for this route.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.
Total delay	Total propagation delay in microseconds.
minimum bandwidth	Minimum bandwidth encountered when transmitting data along this route.
Reliability 255/255	Likelihood of successful packet transmission expressed as a number between 0 and 255 (255 is 100 percent reliability).
minimum MTU	Smallest MTU along the path.
Loading 2/255	Effective bandwidth of the route in kilobits per second/255 is saturation.
Hops	Hops to the destination or to the router where the route first enters IGRP.

The following is sample output using the **longer-prefixes** keyword. When the **longer-prefixes** keyword is included, the address and mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed.

In the following example, the logical AND operation is performed on the source address 128.0.0.0 and the mask 128.0.0.0, resulting in 128.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 128.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 128.0.0.0 128.0.0.0 longer-prefixes

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default

Gateway of last resort is not set

S    134.134.0.0 is directly connected, Ethernet0
S    131.131.0.0 is directly connected, Ethernet0
S    129.129.0.0 is directly connected, Ethernet0
S    128.128.0.0 is directly connected, Ethernet0
S    198.49.246.0 is directly connected, Ethernet0
S    192.160.97.0 is directly connected, Ethernet0
S    192.153.88.0 is directly connected, Ethernet0
S    192.76.141.0 is directly connected, Ethernet0
S    192.75.138.0 is directly connected, Ethernet0
S    192.44.237.0 is directly connected, Ethernet0
S    192.31.222.0 is directly connected, Ethernet0
S    192.16.209.0 is directly connected, Ethernet0
S    144.145.0.0 is directly connected, Ethernet0
S    140.141.0.0 is directly connected, Ethernet0
S    139.138.0.0 is directly connected, Ethernet0
S    129.128.0.0 is directly connected, Ethernet0
S    172.19.0.0 255.255.255.0 is subnetted, 1 subnets
C    172.19.64.0 is directly connected, Ethernet0
S    171.69.0.0 is variably subnetted, 2 subnets, 2 masks
C    171.69.232.32 255.255.255.240 is directly connected, Ethernet0
S    171.69.0.0 255.255.0.0 is directly connected, Ethernet0
Router#
```

The following is sample output from a router configured for Diff-Serv-aware Traffic Engineering:

```
Router-4# show ip route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR

Gateway of last resort is not set

C    2.0.0.0/8 is directly connected, Ethernet0
     24.0.0.0/32 is subnetted, 1 subnets
C    24.1.1.1 is directly connected, Loopback0
     12.0.0.0/24 is subnetted, 1 subnets
C    12.1.1.0 is directly connected, Ethernet1
```

## Related Commands

Command	Description
<b>show interfaces tunnel</b>	Lists tunnel interface information.
<b>show ip route summary</b>	Displays the current state of the routing table in summary format.

# 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 {host {receivers | senders} | installed | interface | neighbor | request |
reservation | sender}
```

Syntax Description	host	Displays RSVP endpoint senders and receivers information.
	<b>installed</b>	Displays RSVP installed reservations.
	<b>interface</b>	Displays RSVP interface information.
	<b>neighbor</b>	Displays RSVP neighbor information.
	<b>request</b>	Displays RSVP reservations upstream information.
	<b>reservation</b>	Displays RSVP reservation requests from downstream.
	<b>sender</b>	Displays RSVP PATH state information.
	<b>temp-psb</b>	Displays RSVP PATH requests awaiting policy decision.
	<b>temp-rsb</b>	Displays RSVP reservation requests awaiting policy decisions.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.0(5)S	The keyword host was added.

**Examples** The following examples show output from **show ip rsvp host receivers** command:

```
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 6 lists the fields displayed in this example.

**Table 6** *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.

**Table 6** *show ip rsvp host Field Descriptions (continued)*

Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit Filter, or Fixed Filter).
Serv	Service (value can be <b>RATE</b> or <b>LOAD</b> ).
BPS	Reservation rate in bits per second.
Bytes	Bytes of burst size requested.

# show ip rsvp interface

To display RSVP-related interface information, use the **show ip rsvp interface** EXEC command.

```
show ip rsvp interface [interface-type interface-number]
```

Syntax Description	Parameter	Description
	<i>interface-type</i>	(Optional) The name of the interface.
	<i>interface-number</i>	(Optional) The number of the interface.

**Command Modes** EXEC

Command History	Release	Modification
	11.2	This command was introduced.

**Usage Guidelines** Use this command to show the current allocation budget and maximum allocatable bandwidth.

**Examples** The following is sample output from the **show ip rsvp interface** command:

```
Router# show ip rsvp interface

interfac allocate i/f max  flow max per/255 UDP  IP  UDP_IP  UDP M/C
Et1      0M      7500K  7500K  0 /255 0   0   0      0
Se0      0M      1158K  1158K  0 /255 0   0   0      0
Se1      30K      1158K  1158K  6 /255 0   1   0      0
```

Table 7 describes significant fields shown in this display.

**Table 7** *show ip rsvp interface* Field Descriptions

Field	Description
interface	Interface name.
allocate	Current allocation budget.
i/f max	Maximum allocatable bandwidth.
flow max	Maximum flow possible on this interface.
per /255	Percent of bandwidth utilized.
UDP	Number of neighbors sending UDP-encapsulated RSVP.
IP	Number of neighbors sending IP-encapsulated RSVP.
UDP_IP	Number of neighbors sending both UDP- and IP-encapsulated RSVP.
UDP M/C	Is router configured for UDP on this interface?

## ■ show ip rsvp interface

The following is sample output from a router configured for Diff-Serv-aware Traffic Engineering:

```
Router-3# show ip rsvp interface
interface    allocated  i/f max  flow max  gtd UDP  IP      UDP_IP  UDP M/C
Et1          0M         1M       1M        1628239120 0    1      0      0
Hs0          0M         10K      10K       1628239120 0    0      0      0
```

# show mpls traffic-eng autoroute

To show tunnels that are announced to 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 IGP's enhanced SPF (shortest path first) calculation has been modified to understand traffic engineering tunnels. This command shows which tunnels are currently being used by the IGP in its enhanced SPF calculation (tunnels that 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 will 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 8 lists the fields displayed in this example.

**Table 8** *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 8** *show mpls traffic-eng autoroute Field Descriptions*

<b>Field</b>	<b>Description</b>
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**

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

# show mpls traffic-eng fast-reroute database

To display the contents of the Fast Reroute database, use the **show mpls traffic-eng fast-reroute database EXEC** command.

```

show mpls traffic-eng fast-reroute database
  [{network [mask | masklength]
  | labels low label [-high label] |
  interface ifname [ backup-interface ifname ] |
  backup-interface ifname}]
  [state {active | ready | partial}]
  [role {head | middle}]
  [detail]

```

Syntax	Description
<i>network</i>	IP address of the destination network. This functions as the prefix of the Fast Reroute rewrite.
<i>mask</i>	Bit combination indicating the portion of the IP address that is being used for the subnet address.
<i>masklength</i>	Number of bits in mask of destination.
<b>labels</b>	Shows only database entries that possess in-labels assigned by this router (local labels). You specify either a starting value or a range of values.
<i>low label</i>	Starting label value or lowest value in the range.
<i>- high label</i>	Highest label value in the range.
<b>interface</b>	Shows only database entries related to the primary outgoing interface.
<i>ifname</i>	Name of the primary outgoing interface.
<b>backup-interface</b>	Shows only database entries related to the backup outgoing interface.
<i>ifname</i>	Name of the backup outgoing interface.
<b>state</b>	Shows entries that match one of four possible states: partial, complete, ready, or active.
<b>partial</b>	State before the FRR rewrite has been fully created; its backup routing information is still incomplete.
<b>complete</b>	State after the FRR rewrite has been assembled: it is either ready or active.
<b>ready</b>	The FRR rewrite has been created, but has not yet been moved into the forwarding database.
<b>active</b>	The FRR rewrite has been put into the forwarding database (where it can be placed onto appropriate incoming packets).
<b>role</b>	Shows entries associated either with the tunnel head or tunnel midpoint.
<b>head</b>	Entry associated with tunnel head.
<b>middle</b>	Entry associated with tunnel midpoint.
<b>detail</b>	Shows long-form information: LFIB-FRR total number of clusters, groups and items (defined in Table 10 on page 67) in addition to the short-form information of prefix, label and state.

## show mpls traffic-eng fast-reroute database

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	12.0(10)ST	This command was introduced.

**Examples** The following example shows output from the **show mpls traffic-eng fast-reroute database** command at a tunnel head link.

```
router# show mpls traffic-eng fast-reroute database 12.0.0.0
Tunnel head fast reroute information:
Prefix      Tunnel  In-label  Out intf/labelFRR intf/labelStatus
12.0.0.0/16Tu111  Tun hd  PO0/0:UntaggedTu4000:16  ready
12.0.0.0/16Tu449  Tun hd  PO0/0:UntaggedTu4000:736  ready
12.0.0.0/16Tu314  Tun hd  PO0/0:UntaggedTu4000:757  ready
12.0.0.0/16Tu313  Tun hd  PO0/0:UntaggedTu4000:756  ready
```

**Table 9 Description of fields in show MPLS traffic-eng fast-reroute database**

Field	Description
Prefix	Address to which packets with this label are going.
Tunnel	Tunnel's identifying number.
In Label	Label advertised to other routers to signify a particular prefix. The value "Tunnel head" occurs when no such label has been advertised.
Out intf/ label	Out interface—short name of the physical interface through which traffic goes to the protected link.  Out label: —At a tunnel head, this is the label advertised by the tunnel destination device. The value "Untagged" occurs when no such label has been advertised. —At tunnel midpoints, this is the label selected by the next hop device. The "Pop Tag" value occurs when the next hop is the tunnel's final hop.
FRR intf/ label	Fast Reroute interface—the backup tunnel interface.  Fast Reroute label —At a tunnel head, this is the label selected by the tunnel tail to indicate the destination network. The value "Untagged" occurs when no such label has been advertised. —At tunnel midpoints, this has the same value as the Out Label.
Status	State of the rewrite: partial, ready, or active. (These terms are defined above, in the Syntax Description section).

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **labels** argument specified at a midpoint link:

```
Router# show mpls traffic-eng fast-reroute database labels 250 - 255
Tunnel head fast reroute information:
Prefix Tunnel      In-label Out intf/label   FRR intf/label   Status

LSP midpoint frr information:
LSP identifier      In-label Out intf/label   FRR intf/label   Status
10.110.0.10 229 [7334] 255 P00/0:694 Tu4000:694 active
10.110.0.10 228 [7332] 254 P00/0:693 Tu4000:693 active
10.110.0.10 227 [7331] 253 P00/0:692 Tu4000:692 active
10.110.0.10 226 [7334] 252 P00/0:691 Tu4000:691 active
10.110.0.10 225 [7333] 251 P00/0:690 Tu4000:690 active
10.110.0.10 224 [7329] 250 P00/0:689 Tu4000:689 active
```

The following example shows output from the **show mpls traffic-eng fast-reroute database** command with the **detail** argument included at a tunnel head link:

```
Router# show mpls traffic-eng fast-reroute database 12.0.0.0. detail
LFIB FRR Database Summary:
  Total Clusters:      2
  Total Groups:        2
  Total Items:         789
Link 10:PO5/0 (Down, 1 group)
  Group 51:PO5/0->Tu4000 (Up, 779 members)
    Prefix 12.0.0.0/16, Tu313, active
      Input label Tun hd, Output label P00/0:773, FRR label Tu4000:773
    Prefix 12.0.0.0/16, Tu392, active
      Input label Tun hd, Output label P00/0:775, FRR label Tu4000:775
    Prefix 12.0.0.0/16, Tu111, active
      Input label Tun hd, Output label P00/0:16, FRR label Tu4000:16
    Prefix 12.0.0.0/16, Tu394, active
      Input label Tun hd, Output label P00/0:774, FRR label Tu4000:774
```

**Table 10** Description of fields when detail keyword is used with show MPLS traffic-eng fast-reroute database

Field	Description
Total Clusters	A cluster is the physical interface upon which Fast Reroute link protection has been enabled.
Total Groups	A group is a database record that associates the link-protected physical interface with a backup tunnel. A cluster (physical interface) therefore can have one or more groups.  For example, the cluster Ethernet4/0/1 is protected by backup Tunnel1 and backup Tunnel2, and so has two groups.
Total Items	An item is a database record that associates a rewrite with a group. A group therefore can have one or more items.

■ show mpls traffic-eng fast-reroute database

Field	Description
Link 10:PO5/0 (Down, 1 group)	<p>This describes a cluster (physical interface):</p> <ul style="list-style-type: none"> <li>• "10" is the interface's unique IOS-assigned ID number.</li> <li>• ":" is followed by the interface's short name.</li> <li>• Parentheses contain the operating state of the interface (Up or Down) and the number of groups associated with it.</li> </ul>
Group 51:PO5/0->Tu4000 (Up, 779 members)	<p>This describes a group:</p> <ul style="list-style-type: none"> <li>• "51" is the ID number of the backup interface.</li> <li>• ":" is followed by the group's physical interface short name.</li> <li>• "-&gt;" is followed by the backup tunnel interface short name.</li> <li>• Parentheses contain the operating state of the tunnel interface (Up or Down) and the number of items—also called “members”—associated with it.</li> </ul>

#### Related Commands

Command	Description
show mpls traffic-eng fast-reroute log reroutes	Displays contents of Fast Reroute event log.

# show mpls traffic-eng fast-reroute log reroutes

To display the contents of the Fast Reroute event log, use the **show mpls traffic-eng fast-reroute log reroutes EXEC** command.

```
show mpls traffic-eng fast-reroute log reroutes
```

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	12.0(10)ST	This command was introduced.

**Examples** The following example shows output from the **show mpls traffic-eng fast-reroute log reroutes** command.

```
router# show mpls traffic-eng fast-reroute log reroutes
When      Interface Event  Rewrites Duration CPU msecs Suspend Errors
00:27:39 P00/0   Down  1079   30 msec 30      0      0
00:27:35 P00/0   Up    1079   40 msec 40      0      0
```

**Table 11 Description of Display Fields in show mpls traffic-eng fast-reroute log reroutes**

Display Field	Description
When	Indicates how long ago the logged event occurred (before this line was displayed on your screen). Displayed as hours, minutes, seconds.
Interface	The physical or tunnel interface where the logged event occurred.
Event	The change to Up or Down by the affected interface.
Rewrites	Total number of reroutes accomplished because of this event.
Duration	Time elapsed during the rerouting process.
CPU msecs	CPU time spent processing those reroutes. (This is less than or equal to the Duration value).
Suspend	Number of times that reroute processing for this event was interrupted to let the CPU handle other tasks.
Errors	Number of unsuccessful reroute attempts.

Related Commands	Command	Description
	<b>show mpls traffic-eng fast-reroute database</b>	Displays contents of Fast Reroute database.

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

To show which tunnels have been 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** command in EXEC mode.

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

<b>Syntax Description</b>	<b>interface name</b> (Optional) Shows only those tunnels that are admitted on the specified interface.
---------------------------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	EXEC
----------------------	------

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.

**Examples** The following example shows output from the **show mpls traffic-eng link-management admission-control** command:

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

```
System Information::
  Tunnels Count:      1
  Tunnels Selected:   1
TUNNEL ID            UP IF      DOWN IF  PRIORITY STATE          BANDWIDTH
3.3.25.3 1_1        -        PO1/0/0  1/1      Resv Admitted  10000      R
```

Table 12 lists the fields displayed in this example.

**Table 12** *show mpls traffic-eng link-management admission-control Field Descriptions*

<b>Field</b>	<b>Description</b>
Tunnels Count	Total number of tunnels admitted.
Tunnels Selected	Number of tunnels to be displayed.
TUNNEL ID	Tunnel identification.
UP IF	Upstream interface used by the tunnel.
DOWN IF	Downstream interface used by the tunnel.
PRIORITY	Setup priority of the tunnel, followed by the hold priority.

**Table 12** *show mpls traffic-eng link-management admission-control Field Descriptions*

STATE	Admission status of the table.
BANDWIDTH	Bandwidth in bits per second. If an “R” appears after the bandwidth number, it means the bandwidth has been reserved. If an “H” appears after the bandwidth number, it means the bandwidth has been temporarily held for a path message.

**Related Commands**

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

# show mpls traffic-eng link-management advertisements

To show local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology, use the **show mpls traffic-eng link-management advertisements** command in EXEC mode.

## 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.

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

```
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:    10.32.0.6
    IGP Neighbor:      ID 0001.0000.0002.00, IP 10.32.0.10
    Admin. Weight:     10
    Physical BW:       155520000 bits/sec
    Reservable BW:     5000000 bits/sec
  Output Bandwidth::
    BW Unreserved[0]:  5000000 bits/sec
    BW Unreserved[1]:  1000000 bits/sec
    BW Unreserved[2]:  1000000 bits/sec
    BW Unreserved[3]:  1000000 bits/sec
    BW Unreserved[4]:  1000000 bits/sec
    BW Unreserved[5]:  1000000 bits/sec
    BW Unreserved[6]:  1000000 bits/sec
    BW Unreserved[7]:  1000000 bits/sec
  Affinity Bits       0x00000000
```

Table 13 lists the fields displayed in this example.

**Table 13** *show mpls traffic-eng link-management advertisements Field Descriptions*

Field	Description
Flooding Status	Enable 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 being used to flood information for this area.
IGP System ID	Identification used by IGP flooding this area to identify this node.
MPLS TE Router ID	MPLS traffic engineering router ID.
Flooded Links	Number of links flooded for this area.
Link ID	Index of the link 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 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 being flooded.

The following is sample output from a router configured for Diff-Serv-aware Traffic Engineering:

```

router2 > show mpls traffic-eng link-management advertisements
Flooding Status:      ready
Configured Areas:    1
IGP Area[1] ID::    ospf area 0
  System Information::
    Flooding Protocol:  OSPF
  Header Information::
    IGP System ID:      24.1.1.1
    MPLS TE Router ID:  24.1.1.1
    Flooded Links:      1
Link ID:: 0
  Link IP Address:      12.1.1.3
  IGP Neighbor:         ID 12.1.1.3, IP 12.1.1.3
  Admin. Weight:        10
  Physical Bandwidth:   10000 kbits/sec
  Max Reservable BW:    1000 kbits/sec
  Reservable GTD BW:    0 kbits/sec
  Downstream::
                                Best-effort  Guaranteed
                                -----
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Reservable Bandwidth 1000  0 kbits/sec
  Attribute Flags:      0x00000000

```

## ■ show mpls traffic-eng link-management advertisements

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>show mpls traffic-eng link-management advertisements</b>	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
	<b>show mpls traffic-eng link-management bandwidth-allocation</b>	Displays current local link information.
	<b>show mpls traffic-eng link-management igp-neighbors</b>	Displays IGP neighbors.
	<b>show mpls traffic-eng link-management interfaces</b>	Displays per-interface resource and configuration information.
	<b>show mpls traffic-eng link-management summary</b>	Displays 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** command in EXEC mode.

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

<b>Syntax Description</b>	<b>interface name</b>	(Optional) Shows only those tunnels that have been admitted on the specified interface.
<b>Defaults</b>	No default behavior or values.	
<b>Command Modes</b>	EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
<b>Usage Guidelines</b>	Advertised information may differ from current information depending on how flooding has been configured.	

**Examples**

The following example shows output from this command:

```
show mpls traffic-eng link-management bandwidth-allocation atm0/0.1

System Information::
  Links Count:          3
  Bandwidth Hold Time: max. 15 seconds
Link ID:: AT0/0.1 (10.32.0.6)
Link Status:
  Physical Bandwidth:  155520000 bits/sec
  MPLS TE Bandwidth:  5000000 bits/sec (reserved:0% in, 80% out)
  BW Descriptors:     1
  MPLS TE Link State: MPLS TE on, RSVP on, admin-up, flooded
  Inbound Admission:  allow-all
  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)
Outbound Bandwidth Information (bits/second):
  KEEP PRIORITY    BW HELD    BW TOTAL HELD    BW LOCKED    BW TOTAL LOCKED
                   0           0                 0             0
                   1           0                 4000000       4000000
                   2           0                 0             4000000
                   3           0                 0             4000000
                   4           0                 0             4000000
                   5           0                 0             4000000
                   6           0                 0             4000000
                   7           0                 0             4000000
```

Table 14 lists the fields displayed in this example.

**Table 14** *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	Bandwidth hold time of the link in seconds.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Bandwidth capacity of the link (in bits per second).
MPLS TE Bandwidth	Amount of reservable bandwidth on this link.
BW Descriptors	Number of bandwidth allocations on this link.
MPLS TE Link State	Status of the MPLS traffic engineering-related functions of the link.
Inbound Admission	Admission policy of the link for incoming tunnels.
Outbound Admission	Admission policy of the link for outgoing tunnels.
Admin. Weight	Administrative weight associated with this link.
Up Thresholds	Bandwidth thresholds of the link for allocations.
Down Thresholds	Bandwidth thresholds of the link for deallocations.
IGP Neighbor	List of the IGP neighbors directly reachable over this link.
KEEP PRIORITY	Priority levels for the bandwidth allocations of the link.
BW HELD	Amount of bandwidth (in bits per seconds) temporarily held at this priority for path messages.
BW TOTAL HELD	Bandwidth held at this priority and those above it.

**Table 14** show mpls traffic-eng link-management bandwidth-allocation Field Descriptions

BW LOCKED	Amount of bandwidth reserved at this priority.
BW TOTAL LOCKED	Bandwidth reserved at this priority and those above.

The following is sample output from a router configured for Diff-Serv-aware Traffic Engineering:

```
router-2> show mpls traffic-eng link-management bandwidth-allocation
System Information::
  Links Count:          1
  Bandwidth Hold Time: max. 15 seconds
Link ID:: Et1 (12.1.1.3)
Link Status:
  Physical Bandwidth:  10000 kbits/sec
  MPLS BE Bandwidth:   1000 kbits/sec (reserved: 0% in, 0% out)
  MPLS GTD Bandwidth:  0 kbits/sec (reserved: 100% in, 100% out)
  Max Reservable BW:   1000 kbits/sec (reserved: 0% in, 0% out)
  BW Descriptors:      0
  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 BE Bandwidth Information (kbits/sec):
  KEEP PRIORITY      BW HELD  BW TOTAL HELD  BW LOCKED  BW TOTAL LOCKED
  0                   0         0             0           0
  1                   0         0             0           0
  2                   0         0             0           0
  3                   0         0             0           0
  4                   0         0             0           0
  5                   0         0             0           0
  6                   0         0             0           0
  7                   0         0             0           0
Downstream GTD Bandwidth Information (bits/second):
  KEEP PRIORITY      BW HELD  BW TOTAL HELD  BW LOCKED  BW TOTAL LOCKED
  0                   0         0             0           0
  1                   0         0             0           0
  2                   0         0             0           0
  3                   0         0             0           0
  4                   0         0             0           0
  5                   0         0             0           0
  6                   0         0             0           0
  7                   0         0             0           0
```

Related Commands	Command	Description
	<b>show mpls traffic-eng link-management advertisements</b>	Displays local link information currently being flooded by MPLS traffic engineering link management into the global traffic engineering topology.
	<b>show mpls traffic-eng link-management bandwidth-allocation</b>	Displays current local link information.

## ■ show mpls traffic-eng link-management bandwidth-allocation

<b>Command</b>	<b>Description</b>
<b>show mpls traffic-eng link-management igp-neighbors</b>	Displays IGP neighbors.
<b>show mpls traffic-eng link-management interfaces</b>	Displays per-interface resource and configuration information.
<b>show mpls traffic-eng link-management summary</b>	Displays summary of link management information.

# show mpls traffic-eng link-management igp-neighbors

To show IGP (Interior Gateway Protocol) 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 using a specified IGP identification.
	isis <i>isis-address</i>	Specifies an IS-IS neighbor to display when displaying neighbors by IGP ID.
	ospf <i>ospf-id</i>	Specifies an OSPF neighbor to display when displaying neighbors by IGP ID.
	ip <i>A.B.C.D</i>	Shows the IGP neighbors 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 15 lists the fields displayed in this example.

**Table 15** *show mpls traffic-eng link-management igp-neighbors* Field Descriptions

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

**show mpls traffic-eng link-management igp-neighbors**

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

# show mpls traffic-eng link-management interfaces

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

```
show mpls traffic-eng link-management interfaces [interface]
```

<b>Syntax Description</b>	<i>interface</i>	(Optional) Specifies the name of a single interface for which information is to be displayed.
<b>Defaults</b>	No default behavior or values.S	
<b>Command Modes</b>	EXEC	
<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.

## Examples

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

```
show mpls traffic-eng link-management interfaces
```

```
System Information::
Links Count:          3
Link ID:: Et1/1/1 (10.1.0.6)
  Link Status:
    Physical Bandwidth: 10000000 bits/sec
    MPLS TE Bandwidth: 5000000 bits/sec (reserved:0% in, 0% out)
    MPLS TE Link State: MPLS TE on, RSVP on
    Inbound Admission:  reject-huge
    Outbound Admission: allow-if-room
    Admin. Weight:      10 (IGP)
    IGP Neighbor Count: 2
    IGP Neighbor:       ID 0000.0000.0000.02, IP 0.0.0.0 (Up)
    IGP Neighbor:       ID 0001.0000.0001.02, IP 0.0.0.0 (Down)
  Flooding Status for each configured area [1]:
    IGP Area[1] isis level-1: not flooded
    (Reason:Interface has been administratively disabled)
Link ID:: AT0/0.1 (10.32.0.6)
  Link Status:
    Physical Bandwidth: 155520000 bits/sec
    MPLS TE Bandwidth: 5000000 bits/sec (reserved:0% in, 80% out)
    MPLS TE Link State: MPLS TE on, RSVP on, admin-up, flooded
    Inbound Admission:  allow-all
    Outbound Admission: allow-if-room
    Admin. Weight:      10 (IGP)
    IGP Neighbor Count: 1
    IGP Neighbor:       ID 0001.0000.0002.00, IP 10.32.0.10 (Up)
  Flooding Status for each configured area [1]:
    IGP Area[1] isis level-1: flooded
```

Table 16 lists the fields displayed in this example.

**Table 16** *show mpls traffic-eng link-management interfaces Field Descriptions*

<b>Field</b>	<b>Description</b>
Links Count	Number of links that have been enabled for use with MPLS traffic engineering.
Physical Bandwidth	Bandwidth capacity of the link (in bits per second).
MPLS TE Bandwidth	Amount of reservable bandwidth on this link.
MPLS TE Link State	The status of the MPLS link.
Inbound Admission	Admission policy for a link for incoming tunnels.
Outbound Admission	Admission policy for a link for outgoing tunnels.
Admin. Weight	Administrative weight associated with this link.
IGP Neighbor Count	Number of IGP neighbors directly reachable over this link.
IGP Area [1]	Flooding status for the specified configured area.

#### **Related Commands**

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

# show mpls traffic-eng link-management summary

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

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

<b>Syntax Description</b>	<i>interface name</i> (Optional) Specifies the name of a single interface for which information is to be displayed.				
<b>Defaults</b>	No default behavior or values.				
<b>Command Modes</b>	EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.0(5)S</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.0(5)S	This command was introduced.
Release	Modification				
12.0(5)S	This command was introduced.				

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

```
show mpls traffic-eng link-management summary atm0/0.1

System Information::
  Links Count:          3
  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:      3
Link ID:: AT0/0.1 (10.32.0.6)
Link Status:
  Physical Bandwidth:  155520000 bits/sec
  MPLS TE Bandwidth:  5000000 bits/sec (reserved:0% in, 80% out)
  MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
  Inbound Admission:  allow-all
  Outbound Admission: allow-if-room
  Admin. Weight:      10 (IGP)
  IGP Neighbor Count: 1
```

Table 17 lists the fields displayed in this example.

**Table 17** *show mpls traffic-eng link-management summary Field Descriptions*

<b>Field</b>	<b>Description</b>
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 flooded.
IGP System ID	IGP for the 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	Bandwidth capacity for the link (in bits per second).
MPLS TE Bandwidth	Amount of reservable bandwidth on this link.
MPLS TE Link State	Status of the MPLS traffic engineering-related functions of the link.
Inbound Admission	Admission policy of the link for incoming tunnels.
Outbound Admission	Admission policy of the link for outgoing tunnels.
Admin. Weight	Administrative weight of the link.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.

**Related Commands**

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

# show mpls traffic-eng topology

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

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

Syntax Description		
<i>A.B.C.D</i>		Specifies the node by the IP address (router identifier to interface address).
<b>igp-id</b>		Specifies the node by IGP router identifier.
<b>isis nsapaddr</b>		Specifies the node by router identification (nsapaddr) if using IS-IS.
<b>ospf A.B.C.D</b>		Specifies the node by router identifier if using OSPF.
<b>brief</b>		(Optional) The 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.
	12.0(11)ST	The single “Reservable” column was replaced by two columns: one each for “global pool” and for “sub-pool”.

**Examples** The following example shows output from the **show mpls traffic-eng topology** command:

```
show mpls traffic-eng topology

My_System_id: 0000.0025.0003.00

IGP Id: 0000.0024.0004.00, MPLS TE Id:24.4.4.4 Router Node
  link[0 ]:Intf Address: 150.1.1.4
             Nbr IGP Id: 0000.0024.0004.02,
             admin_weight:10, affinity_bits:0x0
             max_link_bw:10000 max_link_reservable: 10000
             globalpool  subpool
             total allocated reservable  reservable
             -----
bw[0]:      0           1000           500
bw[1]:      10          990           490
bw[2]:      600         390           390
bw[3]:      0           390           390
bw[4]:      0           390           390
bw[5]:      0           390           390
```

Table 18 lists the fields displayed in this example.

**Table 18** *show mpls traffic-eng topology Field Descriptions*

<b>Field</b>	<b>Description</b>
My-System_id	Unique identifier of the IGP.
IGP Id	Identification of advertising router.
MPLS TE Id	Unique MPLS traffic engineering identification.
Intf Address	This interface address of the link.
Nbr IGP Id	Neighbor IGP router identifier.
admin_weight	Cost of the link.
affinity_bits	The requirements on the attributes of the links that the traffic crosses.
max_link_bw	Physical line rate.
max_link_reservable	The maximum amount of bandwidth that can be reserved on a link.
total allocated	Amount of bandwidth allocated at that priority.
reservable	Amount of available bandwidth reservable at that priority for each of the two pools, global and sub.

# 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

<i>tunnel_interface</i>	Displays information for the specified tunnelling interface.
<b>brief</b>	(Optional) Displays the information in brief format.
<b>destination</b> <i>address</i>	(Optional) Restricts the display to tunnels destined to the specified IP address.
<b>source-id</b>	Restricts the display to tunnels with a matching source IP address and/or tunnel number.
<i>num</i>	Tunnel number.
<i>ipaddress</i>	Source IP address.
<i>ipaddress num</i>	Source IP address and tunnel number.
<b>role</b>	Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
<b>all</b>	Displays all tunnels.
<b>head</b>	Displays tunnels with their head at this router.
<b>middle</b>	Displays tunnels with a midpoint at this router.
<b>tail</b>	Displays tunnels with a tail at this router.
<b>remote</b>	Displays tunnels with their head at some other router; this is a combination of <b>middle</b> and <b>tail</b> .
<b>up</b>	Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
<b>down</b>	Displays tunnels that are down.
<b>name</b> <i>string</i>	Displays tunnel 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 signalling message so it is available at all hops.
<b>suboptimal constraints none</b>	Displays tunnels whose path metric is greater than the shortest unconstrained path. Selected tunnels have a longer path than the IGP's shortest path.
<b>suboptimal constraints current</b>	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.

## ■ show mpls traffic-eng tunnels

<b>suboptimal constraints max</b>	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.
<b>interface in</b> <i>phys_intf</i>	Displays tunnels that use the specified input interface.
<b>interface out</b> <i>phys_intf</i>	Displays tunnels that use the specified output interface.
<b>interface</b> <i>phys_intf</i>	Displays tunnels that use the specified interface as an input or output interface.
<b>brief</b>	Specifies a format with 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.
12.0(10)ST	The new <b>brief</b> format includes input and output interface information. The <b>suboptimal</b> and <b>interface</b> keywords were added to the non-brief format. The non-brief, non-summary formats contain 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 19 describes the fields displayed in this example.

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

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 19** *Field Descriptions for show mpls traffic-eng tunnels*

<b>Field</b>	<b>Description</b>
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 non-heads, signalled.

**Related Commands**

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

# tunnel destination

To specify the destination for a tunnel interface, use the **tunnel destination** interface configuration command. To remove the destination, use the **no** form of this command.

**tunnel destination** {*hostname* | *ip-address*}

**no tunnel destination**

## Syntax Description

<i>hostname</i>	Name of the host destination.
<i>ip-address</i>	IP address of the host destination expressed in decimal in four-part, dotted notation.

## Defaults

No tunnel interface destination is specified.

## Command Modes

Interface configuration

## Command History

Release	Modification
10.0	This command was introduced.

## Usage Guidelines

You cannot have two tunnels using the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface. Refer to *Network Protocols, Part 2* for more information on AppleTalk Cayman tunneling.

## Examples

The following example enables Cayman tunneling:

```
interface tunnel0
 tunnel source ethernet0
 tunnel destination 131.108.164.19
 tunnel mode cayman
```

The following example enables GRE tunneling:

```
interface tunnel0
 appletalk cable-range 4160-4160 4160.19
 appletalk zone Engineering
 tunnel source ethernet0
 tunnel destination 131.108.164.19
 tunnel mode gre ip
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>appletalk cable-range</b>	Enables an extended AppleTalk network.
<b>appletalk zone</b>	Sets the zone name for the connected AppleTalk network.
<b>tunnel mode</b>	Sets the encapsulation mode for the tunnel interface.
<b>tunnel source</b>	Sets the source address of a tunnel 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** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**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.

Related Commands	Command	Description
	<b>tunnel mpls traffic-eng affinity</b>	Configures tunnel affinity (the properties that the tunnel requires in its links).
	<b>tunnel mpls traffic-eng autoroute announce</b>	Instructs the IGP to use the tunnel in its SPF/next hop calculation (if the tunnel is up).
	<b>tunnel mpls traffic-eng bandwidth</b>	Configures bandwidth required for an MPLS traffic engineering tunnel.
	<b>tunnel mpls traffic-eng path-option</b>	Configures a path option.
	<b>tunnel mpls traffic-eng priority</b>	Configures setup and reservation priority for a tunnel.

# tunnel mpls traffic-eng affinity

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

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

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

Syntax Description		
	<i>properties</i>	Attribute values required for links carrying this tunnel (values of bits are either 0 or 1).
	<b>mask</b> <i>mask</i>	Which attribute values should be checked. If a bit in the mask is 0, a link's attribute value or that bit is irrelevant. If a bit in the masks is 1, the link's attribute value and the tunnel's required affinity for that bit must match.

Defaults	
	<i>properties</i> —0X00000000
	<i>mask</i> —0X0000FFFF

Command Modes	
	Interface configuration

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

**Examples** The following is an example of the **tunnel mpls traffic-eng affinity** command that specifies the attribute value of 1:

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

Related Commands	Command	Description
	<b>mpls traffic-eng attribute-flags</b>	Sets the user-specified attribute-flags for the interface.
	<b>tunnel mode mpls traffic-eng</b>	Sets the mode of a tunnel to MPLS for traffic engineering.

# tunnel mpls traffic-eng autoroute announce

To instruct the IGP to use the tunnel in its SPF/next hop calculation (if the tunnel is up), use the **tunnel mpls traffic-eng autoroute announce** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng autoroute announce**

**no tunnel mpls traffic-eng autoroute announce**

**Syntax Description** This command has no arguments or keywords.

**Defaults** The tunnel is not used by the IGP in its SPF/next hop calculation.

**Command Modes** Interface configuration

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

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

Related Commands	Command	Description
	<b>ip route</b>	Establishes static routes and defines the next hop for large-scale dialout.
	<b>tunnel mode mpls traffic-eng</b>	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 used by IGP autoroute, use the **tunnel mpls traffic-eng autoroute metric** command in interface configuration mode. To disable this feature, use the **no** form of this command.

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

**no tunnel mpls traffic-eng autoroute metric**

Syntax Description	metric	The MPLS traffic engineering tunnel metric.
	<b>absolute</b>	The MPLS traffic-engineering tunnel metric mode absolute: a positive metric value can be supplied.
	<b>relative</b>	The MPLS traffic-engineering tunnel metric mode relative: a positive, negative, or zero value can be supplied.

**Defaults** The default is metric relative 0.

**Command Modes** Interface configuration

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

Related Commands	Command	Description
	<b>show mpls traffic-eng autoroute</b>	Displays tunnels that are announced to IGP, including interface, destination, and bandwidth.
	<b>tunnel mpls traffic-eng autoroute announce</b>	Instructs the IGP to use the tunnel in its SPF/next hop calculation (if the tunnel is up).

## tunnel mpls traffic-eng bandwidth

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

```
tunnel mpls traffic-eng bandwidth {sub-pool | [global]} bandwidth
```

```
no tunnel mpls traffic-eng bandwidth {sub-pool | [global]} bandwidth
```

### Syntax Description

<b>sub-pool</b>	(Optional) Indicates a sub-pool tunnel.
<b>global</b>	(Optional) Indicates a global pool tunnel. Entering this keyword is not necessary, for all tunnels are “global pool” in the absence of the keyword <b>sub-pool</b> . But if users of pre-DS-TE images enter this keyword, it will be accepted.
<i>bandwidth</i>	The bandwidth, in kilobits per second, set aside for the MPLS traffic engineering tunnel. Range is between 1 and 4294967295 .

### Defaults

Default bandwidth is 0.  
Default is a global pool tunnel.

### Command Modes

Interface configuration

### Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(11)ST	Sub-pool option was added.

### Usage Guidelines

Enter the bandwidth for either a global pool or sub-pool tunnel, not both. Only the **ip rsvp bandwidth** command (on page 32) specifies the two bandwidths within one command.

To set up only a global pool tunnel, leave out the keyword **sub-pool**. If you enter **global** as a keyword, the system will accept it, but won't write it to NVRAM. This is to avoid the problem of having one's configuration not understood if one upgrades to an image that contains the DS-TE capability and then returns to a non DS-TE image.

### Related Commands

Command	Description
<b>show mpls traffic-eng tunnel</b>	Displays information about tunnels.

# tunnel mpls traffic-eng fast-reroute

To enable an MPLS traffic engineering tunnel to use a backup tunnel in the event of a link failure if a backup tunnel exists, use the **tunnel mpls traffic-eng fast-reroute** interface configuration command.

## **tunnel mpls traffic-eng fast-reroute**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values.

**Command Modes** Interface

Command History	Release	Modification
	12.0(8)ST	This command was introduced.

**Examples** The following example enables an MPLS traffic engineering tunnel to use a backup tunnel if a link fails and a backup tunnel exists:

```
Router(config_if)# tunnel mpls traffic-eng fast-reroute
```

Related Commands	Command	Description
	<b>mpls traffic-eng backup-path Tunnel</b>	Configures the interface to use a backup tunnel in the event of a detected failure on the interface.
	<b>show tunnel mpls traffic-eng fast-reroute</b>	Displays information about fast reroute for MPLS traffic engineering.

# 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

<i>number</i>	When several path options are configured, lower numbered options are preferred.
<b>dynamic</b>	LSP's path is dynamically calculated.
<b>explicit</b>	LSP's path is an IP explicit path.
<b>name</b> <i>path-name</i>	Path name of the IP explicit path that the tunnel uses with this option.
<i>path-number</i>	Path number of the IP explicit path that the tunnel uses with this option.
<b>lockdown</b>	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 many 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
<b>ip explicit-path</b>	Enters the subcommand mode for IP explicit paths and creates or modifies the specified path.

<b>Command</b>	<b>Description</b>
<b>show ip explicit-paths</b>	Displays the configured IP explicit paths.
<b>tunnel mpls traffic-eng priority</b>	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** command in interface configuration mode. To disable this feature, use the **no** form of this command.

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

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

## Syntax Description

<i>setup-priority</i>	The priority used when signalling an LSP for this tunnel to determine which 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.
<i>hold-priority</i>	(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

The preemption priority mechanism allows a hard-to-fit LSP or a more important LSP to preempt other LSPs so that those other LSPs can be reestablished once the hard-to-fit or more important LSP has been placed.

No distinction is made between sub-pool tunnels and global pool tunnels during preemption: that is, sub-pool tunnels are still preempted by global pool tunnels when the latter possess a higher preemption priority. Similarly, global pool tunnels are preempted by sub-pool tunnels when the latter possess a higher preemption priority. Hence, as sub-pool tunnels typically are more important than global pool tunnels, sub-pool tunnels would typically be configured with higher preemption priority than global pool tunnels.

Typically, setup and hold priorities are configured to be equal. However, a separate hold priority allows a subset of tunnels to not preempt on setup, but to be preempted once established.

Setup priority may not be better than (numerically smaller than) 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
	<b>tunnel mode mpls traffic-eng</b>	Sets the mode of a tunnel to MPLS for traffic engineering.

# Debug Commands

This section documents the following **debug** commands referred to earlier in this feature guide:

- **debug mpls traffic-engineering link-management preemption**

All other MPLS Traffic Engineering debug commands are documented in the Cisco IOS Release 12.1(3)T document entitled *MPLS Traffic Engineering and Enhancements*, which is located at <http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t3/traffeng.htm>

# 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]**

<b>Syntax Description</b>	<b>detail</b> (Optional) Prints detailed debugging information.				
<b>Defaults</b>	No default behavior or values.				
<b>Command Modes</b>	Privileged EXEC				
<b>Command History</b>	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>12.1(3)T</td> <td>This command was introduced.</td> </tr> </tbody> </table>	Release	Modification	12.1(3)T	This command was introduced.
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
```

# Glossary

This section defines acronyms and words that may not be readily understood.

**CBR**—Constraint Based Routing. The computation of traffic paths that simultaneously satisfy label-switched path attributes and current network resource limitations.

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

**CLI**—Command Line Interface. Cisco’s interface for configuring and managing its routers.

**DS-TE**—Diff Serv-aware Traffic Engineering. The capability to configure two bandwidth pools on each link, a *global pool* and a *sub-pool*. MPLS traffic engineering tunnels using the sub-pool bandwidth can be configured with Quality of Service mechanisms to deliver guaranteed bandwidth services end-to-end across the network. Simultaneously, tunnels using the global pool can convey diff-serv traffic.

**flooding**—A traffic passing technique used by switches and bridges in which traffic received on an interface is sent out through all of the interfaces of that device except the interface on which the information was originally received.

**GB queue**—Guaranteed Bandwidth queue. A per-hop behavior (PHB) used exclusively by the strict guarantee traffic. If delay/jitter guarantees are sought, the diffserv Expedited Forwarding queue (EF PHB) is used. If only bandwidth guarantees are sought, the diffserv Assured Forwarding PHB (AF PHB) is used.

**Global Pool**—The total bandwidth allocated to an MPLS traffic engineering link.

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

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

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

**LSP**—Label-switched path (see above).

*Also* Link-state packet—A broadcast packet used by link-state protocols that contains information about neighbors and path costs. LSPs are used by the receiving routers to maintain their routing tables. Also called link-state advertisement (LSA).

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

**MPLS TE**—MPLS Traffic Engineering (formerly known as “RRR” or Resource Reservation Routing). The use of label switching to improve traffic performance along with an efficient use of network resources.

**OSPF**—Open Shortest Path First. A link-state, hierarchical IGP routing algorithm, derived from the IS-IS protocol. OSPF features include least-cost routing, multipath routing, and load balancing.

**RSVP**—Resource reSerVation Protocol. An IETF protocol used for signaling requests (to set aside internet services) by a customer before that customer is permitted to transmit data over that portion of the network.

**Sub-pool**—The more restrictive bandwidth in an MPLS traffic engineering link. The sub-pool is a portion of the link’s overall global pool bandwidth.

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

