



# MPLS Traffic Engineering—DiffServ Aware

---

**First Published:** 12.0(11) ST

**Last Updated:** February 28, 2006

This guide presents extensions made to Multiprotocol Label Switching Traffic Engineering (MPLS TE) that make it DiffServ 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.

## History for the MPLS Traffic Engineering—DiffServ Aware Feature

Release	Modification
12.0(11) ST	This feature was introduced.
12.0(14) ST	Support added for Cisco Series 7500(VIP) platform. Support added for IS-IS Interior Gateway Protocol.
12.0(14) ST-1	Support added for guaranteed bandwidth service directed to many destination prefixes (for example, guaranteed bandwidth service destined to an autonomous system or to a BGP community).
12.0(22)S	This feature integrated into Cisco IOS Release 12.0(22)S.
12.2(28)SB	This feature was integrated into Cisco IOS Release 12.2(28)SB.

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

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



---

Corporate Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2002, 2006 Cisco Systems, Inc. All rights reserved.

# Contents

- [Background and Overview, page 2](#)
- [Prerequisites, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 8](#)
- [Additional References, page 36](#)
- [Command Reference, page 37](#)
- [Glossary, page 152](#)

## 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. DiffServ-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

DiffServ-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, IS-IS, RSVP (Resource reSerVation Protocol), QoS, and MPLS traffic engineering. Cisco documentation for all of these features is listed in the next section.

## Prerequisites

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

- MPLS
- IP Cisco Express Forwarding
- OSPF or ISIS
- RSVP-TE
- QoS

## Configuration Tasks

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

The subsequent “[Configuration Examples](#)” section on page 8 presents these same commands in context and shows how, by combining them with QoS commands, you can build guaranteed bandwidth services.

## Central Commands for DS-TE

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 (router or switch router) to use accelerated packet-forwarding (known as Cisco Express Forwarding), MultiProtocol Label Switching (MPLS), traffic-engineering tunneling, and either the OSPF or IS-IS routing algorithm (Open Shortest Path First or Intermediate System to Intermediate System). 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 distributed</b>	Enables Cisco Express Forwarding—which accelerates the flow of packets through the device.
Step 2	Router(config)# <b>mpls traffic-eng tunnels</b>	Enables MPLS, and specifically its traffic engineering tunnel capability.

	Command	Purpose
Step 3	Router(config)# <b>router ospf</b>  [or] Router(config)# <b>router isis</b>	Invokes the OSPF routing process for IP and puts the device into router configuration mode. Proceed now to Steps 9 and 10.  Alternatively, you may invoke the ISIS routing process with this command, and continue with Step 4.
Step 4	Router (config-router)# <b>net network-entity-title</b>	Specifies the IS-IS network entity title (NET) for the routing process.
Step 5	Router (config-router)# <b>metric-style wide</b>	Enables the router to generate and accept IS-IS new-style TLVs (type, length, and value objects).
Step 6	Router (config-router)# <b>is-type level-n</b>	Configures the router to learn about destinations inside its own area or “IS-IS level”.
Step 7	Router (config-router)# <b>mpls traffic-eng level-n</b>	Specifies the IS-IS level (which must be same level as in the preceding step) to which the router will flood MPLS traffic-engineering link information.
Step 8	Router (config-router)# <b>passive-interface loopback0</b>	Instructs IS-IS to advertise the IP address of the loopback interface without actually running IS-IS on that interface. Continue with Step 9 but don’t do Step 10—because Step 10 refers to OSPF.
Step 9	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.
Step 10	Router(config-router)# <b>mpls traffic-eng area num</b>	Turns on MPLS traffic engineering for a particular OSPF area.

## 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—and if you will be relying on the IS-IS routing protocol, you enable that as well.

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> .
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 <b>sub-pool kbps</b> .

	Command	Purpose
Step 3	Router(config-if)# <b>mpls traffic-eng tunnels</b>	Enables the MPLS traffic engineering tunnel feature on this interface.
Step 4	Router(config-if)# <b>ip router isis</b>	Enables the IS-IS routing protocol on this interface. Do not enter this command if you are configuring for OSPF.

## 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**.

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.
Step 2	Router(config-if)# <b>tunnel destination A.B.C.D</b>	Specifies the IP address of the tunnel tail device.
Step 3	Router(config-if)# <b>tunnel mode mpls traffic-eng</b>	Sets the tunnel’s encapsulation mode to MPLS traffic engineering.
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.
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.
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).

## 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, refer to the **show interfaces tunnel** command and the **show ip rsvp interface** command.

```
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:

```

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.

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

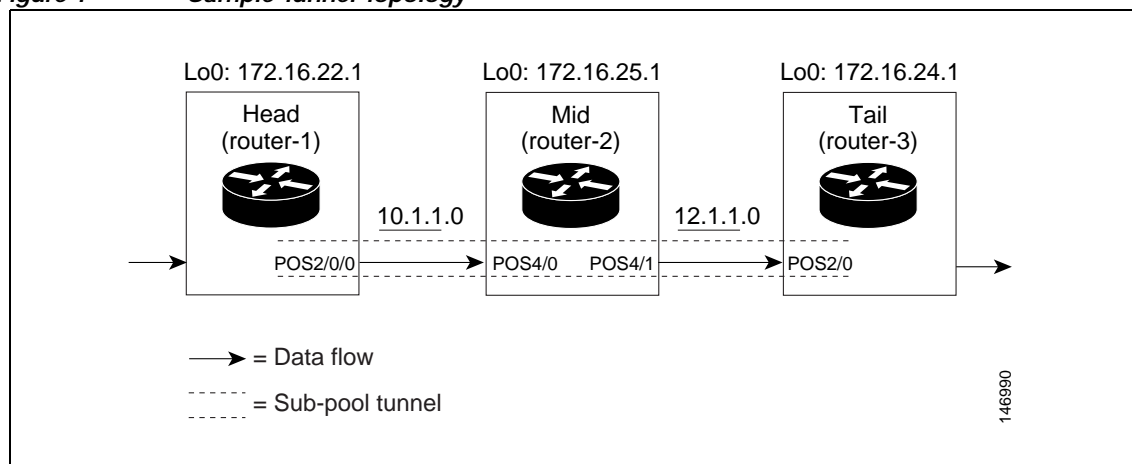
To see information about...		Use this command
this level	and this item...	
Network	Advertised bandwidth allocation information	<b>show mpls traffic-eng link-management advertisements</b>
	Preemptions along the tunnel path	<b>debug mpls traffic-eng link-management preemption</b>
	Available TE link bandwidth on all head routers	<b>show mpls traffic-eng topology</b>
Router	Status of all tunnels currently signalled by this router	<b>show mpls traffic-eng link-management admission-control</b>
	Tunnels configured on midpoint routers	<b>show mpls traffic-eng link-management summary</b>
Physical interface	Detailed information on current bandwidth pools	<b>show mpls traffic-eng link-management bandwidth-allocation [interface-name]</b>
	TE RSVP bookkeeping	<b>show mpls traffic-eng link-management interfaces</b>
	Entire configuration of one interface	<b>show run interface</b>

## Configuration Examples

First this section presents the DS-TE configurations 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.

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 network interfaces must be configured, for traffic ingress and egress.

**Figure 1** *Sample Tunnel Topology*





## Tunnel Head

At the device level:

```
router-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

<pre>router-1(config)# router isis     router-1(config-router)# net 49.0000.1000.0000.0010.00     router-1(config-router)# metric-style wide      router-1(config-router)# is-type level-1      router-1(config-router)# mpls traffic-eng level-1     router-1(config-router)# passive-interface Loopback0</pre>	<pre>router ospf 100 redistribute connected network 10.1.1.0 0.0.0.255 area 0 network 172.16.22.1 0.0.0.0 area 0 mpls traffic-eng area 0</pre>
--	--

[now one resumes the common command set]:

```
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

```
router-1(config)# interface Loopback0
```

At the virtual interface level:

```
router-1(config-if)# ip address 172.16.22.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# exit
```

At the device level:

```
router-1(config)# interface POS2/0/0
```

At the physical interface level (egress):

```
router-1(config-if)# ip address 10.1.1.1 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At the device level:

```
router-1(config)# interface Tunnel1
```

At the tunnel interface level:

```
router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 172.16.24.1
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 30000
router-1(config-if)# tunnel mpls traffic-eng path-option 1 dynamic
router-1(config-if)# exit
router-1(config)#
```

## Midpoint Devices

At the device level:

```
router-2# configure terminal
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

<pre>router-2(config)# router isis router-2(config-router)# net 49.0000.1000.0000.0012.00 router-2(config-router)# metric-style wide  router-2(config-router)# is-type level-1  router-2(config-router)# mpls traffic-eng level-1  router-2(config-router)# passive-interface Loopback0</pre>	<pre>router ospf 100 redistribute connected network 10.0.1.0 0.0.0.255 area 0  network 192.168.12.0 0.0.0.255 area 0  network 172.16.25.1 0.0.0.0 area 0  mpls traffic-eng area 0</pre>
---	---

[now one resumes the common command set]:

```
router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

```
router-2(config)# interface Loopback0
```

At the virtual interface level:

```
router-2(config-if)# ip address 172.16.25.1 255.255.255.255
router-2(config-if)# no ip directed-broadcast
router-2(config-if)# exit
```

At the device level:

```
router-1(config)# interface POS4/0
router-1(config-if)# ip address 10.0.1.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
```

[If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At the device level:

```
router-1(config)# interface POS4/1
router-1(config-if)# ip address 192.168.12.2 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000
```

[If using IS-IS instead of OSPF]:

```
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

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

## Tail-End Device

At the device level:

```

router-3# configure terminal
router-3(config)# ip cef distributed
router-3(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# router isis
    router-3(config-router)# net 49.0000.1000.0000.0013.00
    router-3(config-router)# metric-style wide

    router-3(config-router)# is-type level-1

    router-3(config-router)# mpls traffic-eng level-1
    router-3(config-router)# passive-interface Loopback0
[now one resumes the common command set]:
    router-3(config-router)# mpls traffic-eng router-id Loopback0
    router-3(config-router)# exit

router-3(config)# interface Loopback0

```

At the virtual interface level:

```

router-3(config-if)# ip address 172.16.24.1 255.255.255.255
router-3(config-if)# no ip directed-broadcast
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the device level:

```

router-1(config)# interface POS4/0
router-1(config-if)# ip address 12.1.1.0 255.255.255.0
router-1(config-if)# mpls traffic-eng tunnels
router-1(config-if)# ip rsvp bandwidth 130000 130000 sub-pool 80000

[If using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-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 7500(VIP) it is the "priority" 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 7500 (VIP) you use one of the existing Class-Based Weighted Fair Queuing (CBWFQ) 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 Examples

Given the many topologies in which Guaranteed Bandwidth Services can be applied, there is space here only to present two examples. They illustrate opposite ends of the spectrum of possibilities.

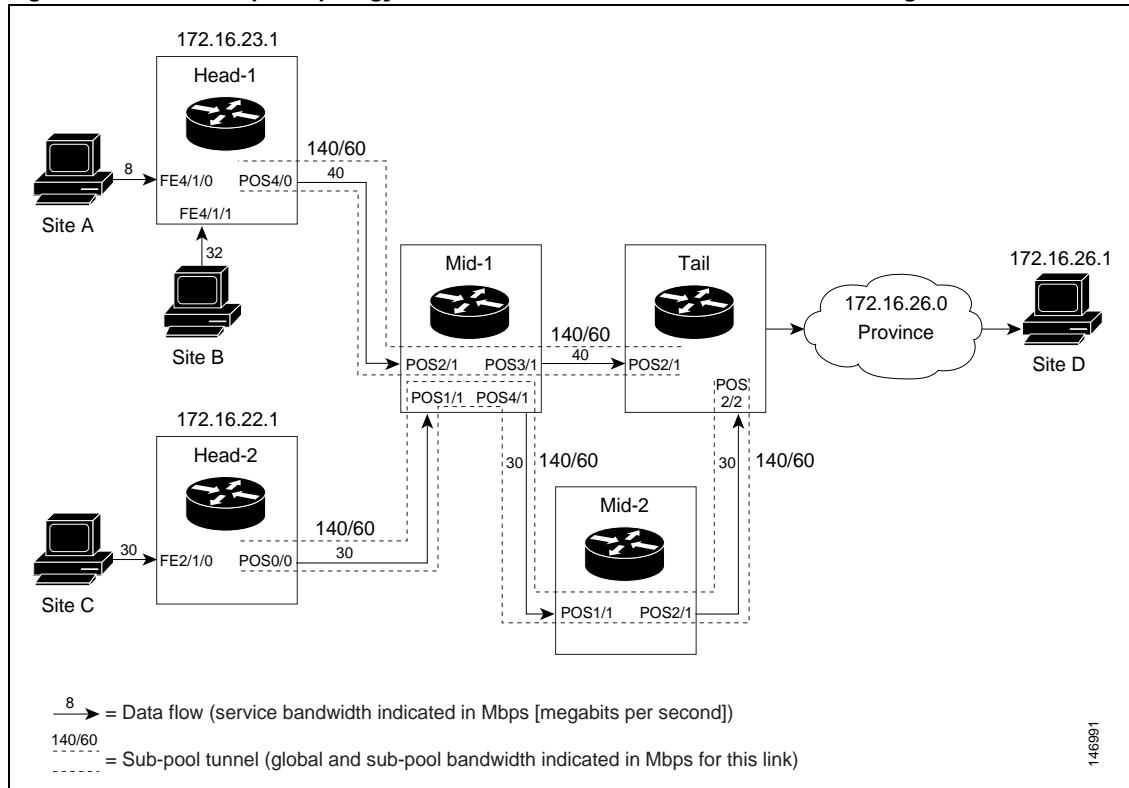
In the first example, the guaranteed bandwidth tunnel can be easily specified by its destination. So the forwarding criteria refer to a single destination prefix.

In the second example, there can be many final destinations for the guaranteed bandwidth traffic, including a dynamically changing number of destination prefixes. So the forwarding criteria are specified by Border Gateway Protocol (BGP) policies.

### Example with Single Destination Prefix

[Figure 2](#) illustrates a topology for guaranteed bandwidth services whose destination is specified by a single prefix, either Site D (like a voice gateway, here bearing prefix 172.16.26.1) or a subnet (like the location of a web farm, here called “Province” and bearing prefix 172.16.26.0). Three services are offered:

- From Site A (defined as all traffic arriving at interface FE4/1/0): to host 172.16.26.1, 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 172.16.26.0, 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 Topology for Guaranteed Bandwidth Services to a Single Destination Prefix

These three services run through two sub-pool tunnels:

- From the Head-1 router, 172.16.23.1, to the router-4 tail
- From the Head-2 router, 172.16.22.1, to the router-4 tail

Both tunnels use the same tail router, though they have different heads. (In Figure 2, one midpoint router is shared by both tunnels. In the real world there could of course be many more midpoints.)

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

## Configuring Tunnel 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. (With the 7500 router, Modular QoS CLI is used.)

### Configuring the Pools and Tunnel

At the device level:

```
router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis                                router ospf 100
router-1(config-router)# net 49.0000.1000.0000.0010.00    redistribute connected
router-1(config-router)# metric-style wide                  network 10.1.1.0 0.0.0.255
                                                            area 0
```

```

router-1(config-router)# is-type level-1
router-1(config-router)# mpls traffic-eng level-1
router-1(config-router)# passive-interface Loopback0
[now one resumes the common command set]:
router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit

```

```

network 172.16.23.1 0.0.0.0
area 0
mpls traffic-eng area 0

```

Create a virtual interface:

```

router-1(config)# interface Loopback0
router-1(config-if)# ip address 172.16.23.1 255.255.255.255
router-1(config-if)# no ip directed-broadcast
router-1(config-if)# 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
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit

```

At the tunnel interface:

```

router-1(config)# interface Tunnel1
router-1(config-if)# bandwidth 110000
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 172.16.27.1
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 172.16.26.1 and subnet 172.16.26.0 are sent into the sub-pool tunnel, we create a static route. At the device level:

```

router-1(config)# ip route 172.16.26.1 255.255.255.0 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 a class of traffic matching ACL 100, called "sla-1-class":

```

class-map match-all sla-1-class
  match access-group 100

```

2. Create an ACL 100 to refer to all packets destined to 172.16.26.1:

```

access-list 100 permit ip any host 172.16.26.1

```

3. Create a policy named "sla-1-input-policy", and according to that policy:

- a. Packets in the class called “sla-1-class” are rate-limited to:
  - a rate of 8 million bits per second
  - a normal burst of 1 million bytes
  - a maximum burst of 2 million bytes
- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.
- c. Packets which exceed this rate are dropped.
- d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-1-input-policy
  class sla-1-class
    police 8000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/1/0.

```
interface FastEthernet4/1/0
  service-policy input sla-1-input-policy
```

#### For Service from Site B to Subnet “Province”

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

1. In global configuration mode, create a class of traffic matching ACL 120, called “sla-2-class”:

```
class-map match-all sla-2-class
  match access-group 120
```

2. Create an ACL, 120, to refer to all packets destined to subnet 172.16.26.0:

```
access-list 120 permit ip any 172.16.26.0 0.0.0.255
```

3. Create a policy named “sla-2-input-policy”, and according to that policy:

- a. Packets in the class called “sla-2-class” are rate-limited to:
  - a rate of 32 million bits per second
  - a normal burst of 1 million bytes
  - a maximum burst of 2 million bytes
- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.
- c. Packets which exceed this rate are dropped.
- d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-2-input-policy
  class sla-2-class
    police 32000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE4/1/1.

```
interface FastEthernet4/1/1
  service-policy input sla-2-input-policy
```



### For Both Services

The outbound interface (POS4/0) is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
  match mpls experimental 5
```

2. Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 62 kbits/sec).

```
policy-map output-interface-policy
  class exp-5-traffic
    priority 32
```

3. The policy is applied to packets exiting interface POS4/0.

```
interface POS4/0
  service-policy output output-interface-policy
```

The result of the above configuration lines is that packets entering the Head-1 router via interface FE4/1/0 destined to host 172.16.26.1, or entering the router via interface FE4/1/1 destined to subnet 172.16.26.0, will have their MPLS experimental bit set to 5. We assume that no other packets entering the router (on any interface) are using this value. (If this cannot be assumed, an additional configuration must be added to mark all such packets to another experimental value.) Packets marked with experimental bit 5, when exiting the router via interface POS4/0, will be placed into the priority 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.

## Configuring Tunnel 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 on the sub-pool tunnel.

### .Configuring the Pools and Tunnel

At the device level:

```
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# router isis                                router ospf 100
router-2(config-router)# net 49.0000.1000.0000.0011.00      redistribute connected
router-2(config-router)# metric-style wide                   network 192.168.11.0
                                                             0.0.0.255 area 0
router-2(config-router)# is-type level-1                    network 172.16.22.1 0.0.0.0
                                                             area 0
router-2(config-router)# mpls traffic-eng level-1           mpls traffic-eng area 0
router-2(config-router)# passive-interface Loopback0
[now one resumes the common command set]:
router-2(config-router)# mpls traffic-eng router-id Loopback0
```

```
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 172.16.22.1 255.255.255.255
router-2(config-if)# no ip directed broadcast
router-2(config-if)# exit
```

At the outgoing physical interface:

```
router-2(config)# interface pos0/0
router-2(config-if)# ip address 192.168.11.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
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 172.16.27.1
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 172.16.26.0 are sent into the sub-pool tunnel, we create a static route, at the device level:

```
router-2(config)# ip route 172.16.26.0 255.255.255.0 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 (FE2/1/0):

1. In global configuration mode, create a class of traffic matching ACL 130, called "sla-3-class":

```
class-map match-all sla-3-class
  match access-group 130
```

2. Create an ACL, 130, to refer to all packets destined to subnet 26.1.1.0:

```
access-list 130 permit ip any 172.16.26.0 0.0.0.255
```

3. Create a policy named "sla-3-input-policy", and according to that policy:

- a. Packets in the class called "sla-3-class" are rate-limited to:
  - a rate of 30 million bits per second
  - a normal burst of 1 million bytes
  - a maximum burst of 2 million bytes
- b. Packets which conform to this rate are marked with MPLS experimental bit 5 and are forwarded.

- c. Packets which exceed this rate are dropped.
- d. All other packets are marked with experimental bit 0 and are forwarded.

```
policy-map sla-3-input-policy
  class sla-3-class
    police 30000000 1000000 2000000 conform-action set-mpls-exp-transmit 5 \
    exceed-action drop
  class class-default
    set-mpls-exp-transmit 0
```

4. The policy is applied to packets entering interface FE2/1/0.

```
interface FastEthernet2/1/0
  service-policy input sla-3-input-policy
```

The outbound interface POS0/0 is configured as follows:

1. In global configuration mode, create a class of traffic matching experimental bit 5, called "exp-5-traffic".

```
class-map match-all exp-5-traffic
  match mpls experimental 5
```

2. Create a policy named "output-interface-policy". According to that policy, packets in the class "exp-5-traffic" are put in the priority queue (which is rate-limited to 32 kbits/sec).

```
policy-map output-interface-policy
  class exp-5-traffic
    priority 32
```

3. The policy is applied to packets exiting interface POS0/0:

```
interface POS0/0
  service-policy output output-interface-policy
```

As a result of all the above configuration lines, packets entering theHead-2 router via interface FE2/1/0 and destined for subnet 172.16.26.0 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 precedence 5 are placed in the priority 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 distributed
router-3(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# <b>router isis</b>	router ospf 100
router-3(config-router)# <b>net 49.0000.2400.0000.0011.00</b>	<b>redistribute connected</b>
router-3(config-router)# <b>metric-style wide</b>	<b>network 10.1.1.0 0.0.0.255</b>
	<b>area 0</b>
router-3(config-router)# <b>is-type level-1</b>	<b>network 192.168.11.0</b>
	<b>0.0.0.255 area 0</b>
router-3(config-router)# <b>mpls traffic-eng level-1</b>	<b>network 172.16.24.1 0.0.0.0</b>
	<b>area 0</b>
router-3(config-router)# <b>passive-interface Loopback0</b>	<b>network 192.168.12.0</b>
	<b>0.0.0.255 area 0</b>
router-3(config-router)#	<b>network 192.168.13.1</b>
	<b>0.0.0.255 area 0</b>
router-3(config-router)#	<b>mpls traffic-eng area 0</b>

[now one resumes the common command set]:

```

router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit

```

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 172.16.24.1 255.255.255.255
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
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 192.168.11.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

At the physical interface level (egress):

```

router-3(config)# interface pos3/1
router-3(config-if)# ip address 192.168.12.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos4/1
router-3(config-if)# ip address 192.168.13.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels

```

```

router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

```

## 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 distributed
router-5(config)# mpls traffic-eng tunnels

```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-5(config)# router isis	router ospf 100
router-5(config-router)# net 49.2500.1000.0000.0012.00	redistribute connected
router-5(config-router)# metric-style wide	network 192.168.13.0
	0.0.0.255 area 0
router-5(config-router)# is-type level-1	network 192.168.14.0
	0.0.0.255 area 0
router-5(config-router)# mpls traffic-eng level-1	network 172.16.25.1 0.0.0.0
	area 0
router-5(config-router)# passive-interface Loopback0	mpls traffic-eng area 0

[now one resumes the common command set]:

```

router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit

```

Create a virtual interface:

```

router-5(config)# interface Loopback0
router-5(config-if)# ip address 172.16.25.1 255.255.255.255
router-5(config-if)# exit

```

At the physical interface level (ingress):

```

router-5(config)# interface pos1/1
router-5(config-if)# ip address 192.168.13.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit

```

At the physical interface level (egress):

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 192.168.14.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

## Tunnel Tail Configuration

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

### Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:
router-4(config)# router isis                                router ospf 100
router-4(config-router)# net 49.0000.2700.0000.0000.00      redistribute connected
router-4(config-router)# metric-style wide                   network 192.168.12.0
                                                             0.0.0.255 area 0
router-4(config-router)# is-type level-1                    network 192.168.14.0
                                                             0.0.0.255 area 0
router-4(config-router)# mpls traffic-eng level-1            network 172.16.27.1 0.0.0.0
                                                             area 0
router-4(config-router)# passive-interface Loopback0        mpls traffic-eng area 0
[now one resumes the common command set]:
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# exit
```

Create a virtual interface:

```
router-4(config)# interface Loopback0
router-4(config-if)# ip address 172.16.27.1 255.255.255.255
router-4(config-if)# exit
```

At the physical interface (ingress):

```
router-4(config)# interface pos2/1
router-4(config-if)# ip address 192.168.12.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 192.168.14.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
```

```
[and in all cases]:  
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.

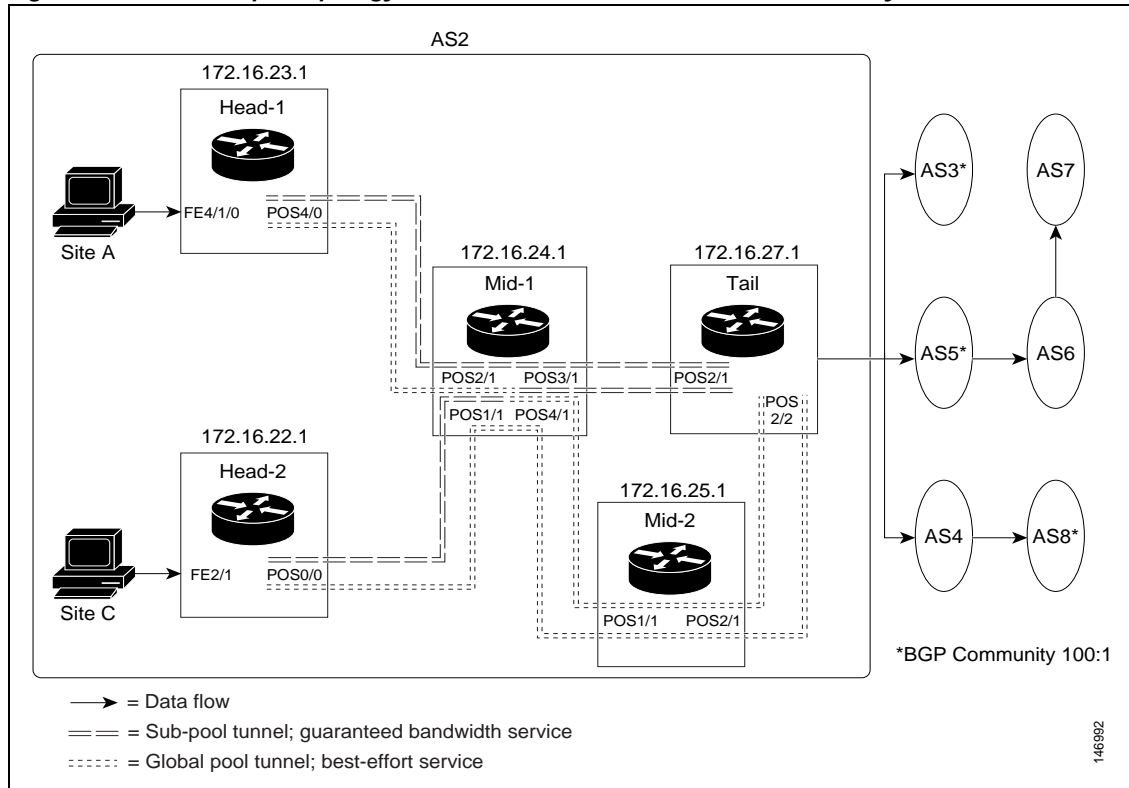
## Example with Many Destination Prefixes

Figure 3 illustrates a topology for guaranteed bandwidth services whose destinations are a set of prefixes. Those prefixes usually share some common properties such as belonging to the same Autonomous System (AS) or transiting through the same AS. Although the individual prefixes may change dynamically because of route flaps in the downstream autonomous systems, the properties the prefixes share will not change. Policies addressing the destination prefix set are enforced through Border Gateway Protocol (BGP), which is described in the following documents:

- “Configuring QoS Policy Propagation via Border Gateway Protocol” section in the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.1
- “Configuring BGP” chapter in the *Cisco IOS IP and IP Routing Configuration Guide*, Release 12.1
- “BGP Commands” chapter in the *Cisco IOS IP and IP Routing Command Reference*, Release 12.1
- “bgp-policy” command in the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.1

In this example, three guaranteed bandwidth services are offered, each coming through a 7500 or a 12000 edge device:

- Traffic coming from Site A (defined as all traffic arriving at interface FE4/1/0) and from Site C (defined as all traffic arriving at interface FE2/1) destined to AS5
- Traffic coming from Sites A and C that transits AS5 but is not destined to AS5. (In the figure, the transiting traffic will go to AS6 and AS7)
- Traffic coming from Sites A and C destined to prefixes advertised with a particular BGP community attribute (100:1). In this example, Autonomous Systems #3, #5, and #8 are the BGP community assigned the attribute 100:1.

**Figure 3** Sample Topology for Guaranteed Bandwidth Service to Many Destination Prefixes

The applicability of guaranteed bandwidth service is not limited to the three types of multiple destination scenarios described above. There is not room in this document to present all possible scenarios. These three were chosen as representative of the wide range of possible deployments.

The guaranteed bandwidth services run through two sub-pool tunnels:

- From the Head-1 router, 172.16.23.1, to the tail
- From the Head-2 router, 172.16.22.1, to that same tail

In addition, a global pool tunnel has been configured from each head end, to carry best-effort traffic to the same destinations. All four tunnels use the same tail router, even though they have different heads and differ in their passage through the midpoints. (Of course in the real world there would be many more midpoints than just the two shown here.)

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

Configuring a multi-destination guaranteed bandwidth service involves:

- Building a sub-pool MPLS-TE tunnel
- Configuring DiffServ QoS
- Configuring QoS Policy Propagation via BGP (QPPB)
- Mapping traffic onto the tunnels

All of these tasks are included in the following example.



## Configuration of Tunnel Head-1

First we recapitulate commands that establish a sub-pool tunnel (commands presented earlier on page 8) and now we also configure a global pool tunnel. Additionally, we present QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (With the 7500(VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

```
router-1(config)# ip cef distributed
router-1(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-1(config)# router isis                                router ospf 100
router-1(config-router)# net 49.0000.1000.0000.0010.00      redistribute connected
router-1(config-router)# metric-style wide                  network 10.1.1.0 0.0.0.255
                                                            area 0
router-1(config-router)# is-type level-1                   network 172.16.23.1 0.0.0.0
                                                            area 0
router-1(config-router)# mpls traffic-eng level-1           mpls traffic-eng area 0

[now one resumes the common command set]:

router-1(config-router)# mpls traffic-eng router-id Loopback0
router-1(config-router)# exit
```

Create a virtual interface:

```
router-1(config)# interface Loopback0
router-1(config-if)# ip address 172.16.23.1 255.255.255.255
router-1(config-if)# 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
[and if using IS-IS instead of OSPF]:
router-1(config-if)# ip router isis
[and in all cases]:
router-1(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-1(config)# interface Tunnel1
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 172.16.27.1
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 explicit name gbs-path1
router-1(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-1(config)# interface Tunnel2
router-1(config-if)# ip unnumbered Loopback0
router-1(config-if)# tunnel destination 172.16.27.1
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 80000
```

```

router-1(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path1
router-1(config-if)# exit

```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```

router-1(config)# ip explicit-path name gbs-path1
router-1(config-ip-expl-path)# next-address 172.16.24.1
router-1(config-ip-expl-path)# next-address 172.16.27.1
router-1(config-ip-expl-path)# exit
router-1(config)# ip explicit-path name best-effort-path1
router-1(config-ip-expl-path)# next-address 172.16.24.1
router-1(config-ip-expl-path)# next-address 172.16.25.1
router-1(config-ip-expl-path)# next-address 172.16.27.1
router-1(config-ip-expl-path)# exit

```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE4/1/0), packets received are rate-limited to:

- a. a rate of 30 Mbps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```

router-1(config)# interface FastEthernet4/1/0
router-1(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-1(config-if)# bgp-policy destination ip-qos-map
router-1(config-if)# exit

```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```

router-1(config)# class-map match-all exp5-class
router-1(config-cmap)# match mpls experimental 5
router-1(config-cmap)# exit

```

Create a policy that creates a priority queue for “exp5-class”:

```

router-1(config)# policy-map core-out-policy
router-1(config-pmap)# class exp5-class
router-1(config-pmap-c)# priority 100000
router-1(config-pmap-c)# exit
router-1(config-pmap)# class class-default
router-1(config-pmap-c)# bandwidth 55000
router-1(config-pmap-c)# exit
router-1(config-pmap)# exit

```

The policy is applied to packets exiting the outbound interface POS4/0.

```

router-1(config)# interface POS4/0
router-1(config-if)# service-policy output core-out-policy

```

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-1(config)# ip bgp-community new-format
router-1(config)# router bgp 2
router-1(config-router)# no synchronization
router-1(config-router)# table-map set-qos-group
router-1(config-router)# bgp log-neighbor-changes
router-1(config-router)# neighbor 172.16.27.1 remote-as 2
router-1(config-router)# neighbor 172.16.27.1 update-source Loopback0
router-1(config-router)# no auto-summary
router-1(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 172.16.29.1 so they will be mapped onto Tunnel #1 (the guaranteed bandwidth service tunnel). At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 100
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 172.16.29.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match as-path 101
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 172.16.29.1
router-1(config-route-map)# exit
router-1(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-1(config)# route-map set-qos-group permit 10
router-1(config-route-map)# match community 20
router-1(config-route-map)# set ip qos-group 6
router-1(config-route-map)# set ip next-hop 172.16.29.1
router-1(config-route-map)# exit
router-1(config)# ip community-list 20 permit 100:1
```

### Mapping Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #1:

```
router-1(config)# ip route 172.16.29.1 255.255.255.255 Tunnel11
```

Map all best-effort traffic onto Tunnel #2:

```
router-1(config)# ip route 172.16.30.1 255.255.255.255 Tunnel12
```

## Configuration of Tunnel Head-2

As with the Head-1 device and interfaces, the following Head-2 configuration first presents commands that establish a sub-pool tunnel (commands presented earlier on page 8) and then also configures a global pool tunnel. After that it presents QoS and BGP commands that guarantee end-to-end service on the sub-pool tunnel. (Because this is a 7500 (VIP) router, Modular QoS CLI is used).

### Configuring the Pools and Tunnels

At the device level:

```
router-2(config)# ip cef distributed
router-2(config)# mpls traffic-eng tunnels
[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-2(config)# router isis                                router ospf 100
router-2(config-router)# net 49.0000.1000.0000.0011.00      redistribute connected
router-2(config-router)# metric-style wide                  network 192.168.11.0
                                                            0.0.0.255 area 0

router-2(config-router)# is-type level-1                   network 172.16.22.1
                                                            0.0.0.0 area 0

router-2(config-router)# mpls traffic-eng level-1           mpls traffic-eng area 0
[now one resumes the common command set]:

router-2(config-router)# mpls traffic-eng router-id Loopback0
router-2(config-router)# exit
```

Create a virtual interface:

```
router-2(config)# interface Loopback0
router-2(config-if)# ip address 172.16.22.1 255.255.255.255
router-2(config-if)# exit
```

At the outgoing physical interface:

```
router-2(config)# interface pos0/0
router-2(config-if)# ip address 192.168.11.1 255.0.0.0
router-2(config-if)# mpls traffic-eng tunnels
router-2(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 60000
[and if using IS-IS instead of OSPF]:
router-2(config-if)# ip router isis
[and in all cases]:
router-2(config-if)# exit
```

At one tunnel interface, create a sub-pool tunnel:

```
router-2(config)# interface Tunnel3
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 172.16.27.1
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 explicit name gbs-path2
router-2(config-if)# exit
```

and at a second tunnel interface, create a global pool tunnel:

```
router-2(config)# interface Tunnel4
router-2(config-if)# ip unnumbered Loopback0
router-2(config-if)# tunnel destination 172.16.27.1
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 70000
router-2(config-if)# tunnel mpls traffic-eng path-option 1 explicit name \
best-effort-path2
router-2(config-if)# exit

```

In this example explicit paths are used instead of dynamic, to ensure that best-effort traffic and guaranteed bandwidth traffic will travel along different paths.

At the device level:

```

router-2(config)# ip explicit-path name gbs-path2
router-2(config-ip-expl-path)# next-address 172.16.24.1
router-2(config-ip-expl-path)# next-address 172.16.27.1
router-2(config-ip-expl-path)# exit
router-2(config)# ip explicit-path name best-effort-path2
router-2(config-ip-expl-path)# next-address 172.16.24.1
router-2(config-ip-expl-path)# next-address 172.16.25.1
router-2(config-ip-expl-path)# next-address 172.16.27.1
router-2(config-ip-expl-path)# exit

```

Note that autoroute is not used, as that could cause the Interior Gateway Protocol (IGP) to send other traffic down these tunnels.

## Configuring DiffServ QoS

At the inbound physical interface (in [Figure 3](#) this is FE2/1), packets received are rate-limited to:

- a. a rate of 30 Mbps
- b. a normal burst of 1 MB
- c. a maximum burst of 2 MB

Packets that are mapped to qos-group 6 and that conform to the rate-limit are marked with experimental value 5 and the BGP destination community string, and are forwarded; packets that do not conform (exceed action) are dropped:

```

router-2(config)# interface FastEthernet2/1
router-2(config-if)# rate-limit input qos-group 6 30000000 1000000 2000000 \
conform-action set-mpls-exp-transmit 5 exceed-action drop
router-2(config-if)# bgp-policy destination ip-qos-map
router-2(config-if)# exit

```

At the device level create a class of traffic called “exp5-class” that has MPLS experimental bit set to 5:

```

router-2(config)# class-map match-all exp5-class
router-2(config-cmap)# match mpls experimental 5
router-2(config-cmap)# exit

```

Create a policy that creates a priority queue for “exp5-class”:

```

router-2(config)# policy-map core-out-policy
router-2(config-pmap)# class exp5-class
router-2(config-pmap-c)# priority 100000
router-2(config-pmap-c)# exit
router-2(config-pmap)# class class-default
router-2(config-pmap-c)# bandwidth 55000
router-2(config-pmap-c)# exit
router-2(config-pmap)# exit

```

The policy is applied to packets exiting interface POS0/0:

```

interface POS0/0
 service-policy output core-out-policy

```

As a result of all the above configuration lines, packets entering the Head-2 router via interface FE2/1 and destined for AS5, BGP community 100:1, or transiting AS5 will have their experimental field set to 5. It is assumed that no other packets entering this router (on any interface) are using this exp bit value. (If this cannot be assumed, an additional configuration must be added to mark all such packets with another experimental value.) When exiting this router via interface POS0/0, packets marked with experimental value 5 are placed into the priority queue.

**Note**

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

## Configuring QoS Policy Propagation via BGP

### For All GB Services

Create a table map under BGP to map (tie) the prefixes to a qos-group. At the device level:

```
router-2(config)# ip bgp-community new-format
router-2(config)# router bgp 2
router-2(config-router)# no synchronization
router-2(config-router)# table-map set-qos-group
router-2(config-router)# bgp log-neighbor-changes
router-2(config-router)# neighbor 172.16.27.1 remote-as 2
router-2(config-router)# neighbor 172.16.27.1 update-source Loopback0
router-2(config-router)# no auto-summary
router-2(config-router)# exit
```

### For GB Service Destined to AS5

Create a distinct route map for this service. This includes setting the next-hop of packets matching 29.1.1.1 so they will be mapped onto Tunnel #3 (the guaranteed bandwidth service tunnel). At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 100
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 172.16.29.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 100 permit ^5$
```

### For GB Service Transiting through AS5

Create a distinct route map for this service. (Its traffic will go to AS6 and AS7).

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
router-2(config-route-map)# match as-path 101
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 172.16.29.1
router-2(config-route-map)# exit
router-2(config)# ip as-path access-list 101 permit _5_
```

### For GB Service Destined to Community 100:1

Create a distinct route map for all traffic destined to prefixes that have community value 100:1. This traffic will go to AS3, AS5, and AS8.

At the device level:

```
router-2(config)# route-map set-qos-group permit 10
```

```

router-2(config-route-map)# match community 20
router-2(config-route-map)# set ip qos-group 6
router-2(config-route-map)# set ip next-hop 172.16.29.1
router-2(config-route-map)# exit
router-2(config)# ip community-list 20 permit 100:1

```

### Mapping the Traffic onto the Tunnels

Map all guaranteed bandwidth traffic onto Tunnel #3:

```
router-2(config)# ip route 172.16.29.1 255.255.255.255 Tunnel3
```

Map all best-effort traffic onto Tunnel #4:

```
router-2(config)# ip route 172.16.30.1 255.255.255.255 Tunnel4
```

## Tunnel Midpoint Configuration [Mid-1]

All four interfaces on the midpoint router are configured very much like the outbound interface of the head router. The strategy is to have all mid-point routers in this Autonomous System ready to carry future as well as presently configured sub-pool and global pool tunnels.

### Configuring the Pools and Tunnels

At the device level:

```

router-3(config)# ip cef distributed
router-3(config)# mpls traffic-eng tunnels

```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right]:

router-3(config)# router isis	router ospf 100
router-3(config-router)# net 49.0000.2400.0000.0011.00	redistribute connected
router-3(config-router)# metric-style wide	network 10.1.1.0 0.0.0.255
	area 0
router-3(config-router)# is-type level-1	network 192.168.11.1
	0.0.0.255 area 0
router-3(config-router)# mpls traffic-eng level-1	network 172.16.24.1 0.0.0.0
	area 0
router-3(config-router)#	network 192.168.12.0
	0.0.0.255 area 0
router-3(config-router)#	network 192.168.13.0
	0.0.0.255 area 0
router-3(config-router)#	mpls traffic-eng area 0

[now one resumes the common command set]:

```

router-3(config-router)# mpls traffic-eng router-id Loopback0
router-3(config-router)# exit

```

Create a virtual interface:

```

router-3(config)# interface Loopback0
router-3(config-if)# ip address 172.16.24.1 255.255.255.255
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 70000

```

```
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit

router-3(config)# interface pos1/1
router-3(config-if)# ip address 192.168.11.2 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the physical interface level (egress), through which two sub-pool tunnels currently exit:

```
router-3(config)# interface pos3/1
router-3(config-if)# ip address 192.168.12.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

At the physical interface level (egress), through which two global pool tunnels currently exit:

```
router-3(config)# interface pos4/1
router-3(config-if)# ip address 192.168.13.1 255.0.0.0
router-3(config-if)# mpls traffic-eng tunnels
router-3(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-3(config-if)# ip router isis
[and in all cases]:
router-3(config-if)# exit
```

## Tunnel Midpoint Configuration [Mid-2]

Both interfaces on this midpoint router are configured like the outbound interfaces of the Mid-1 router.

### Configuring the Pools and Tunnels

At the device level:

<pre>router-5(config)# ip cef distributed router-5(config)# mpls traffic-eng tunnels [now one uses either the IS-IS commands on the left or the OSPF commands on the right]:  router-5(config)# router isis     router-5(config-router)# net 49.2500.1000.0000.0012.00     router-5(config-router)# metric-style wide      router-5(config-router)# is-type level-1      router-5(config-router)# mpls traffic-eng level-1      router-5(config-router)# [now one resumes the common command set]:</pre>	<pre>router ospf 100  redistribute connected  network 192.168.13.0  0.0.0.255 area 0   network 192.168.14.0  0.0.0.255 area 0   network 172.16.25.1 0.0.0.0  area 0   mpls traffic-eng area 0</pre>
--	---



```
router-5(config-router)# mpls traffic-eng router-id Loopback0
router-5(config-router)# exit
```

Create a virtual interface:

```
router-5(config)# interface Loopback0
router-5(config-if)# ip address 172.16.25.1 255.255.255.255
router-5(config-if)# exit
```

At the physical interface level (ingress):

```
router-5(config)# interface pos1/1
router-5(config-if)# ip address 192.168.13.2 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

At the physical interface level (egress):

```
router-5(config)# interface pos2/1
router-5(config-if)# ip address 192.168.14.1 255.0.0.0
router-5(config-if)# mpls traffic-eng tunnels
router-5(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-5(config-if)# ip router isis
[and in all cases]:
router-5(config-if)# exit
```

## Tunnel Tail Configuration

The inbound interfaces on the tail router are configured much like the outbound interfaces of the midpoint routers:

### Configuring the Pools and Tunnels

At the device level:

```
router-4(config)# ip cef distributed
router-4(config)# mpls traffic-eng tunnels
```

[now one uses either the IS-IS commands on the left or the OSPF commands on the right. In the case of OSPF, one must advertise two new loopback interfaces—172.16.29.1 and 172.16.30.1 in our example—which are defined in the QoS Policy Propagation section, further along on this page]:

router-4(config)# router isis	router ospf 100
router-4(config-router)# net 49.0000.2700.0000.0000.00	redistribute connected
router-4(config-router)# metric-style wide	network 192.168.12.0
	0.0.0.255 area 0
router-4(config-router)# is-type level-1	network 192.168.14.0
	0.0.0.255 area 0
router-4(config-router)# mpls traffic-eng level-1	network 172.16.27.1 0.0.0.0
	area 0
router-4(config-router)#	network 172.16.29.1 0.0.0.0
	area 0

```

router-4(config-router)#                               network 172.16.30.1 0.0.0.0
                                                         area 0
router-4(config-router)#                               mpls traffic-eng area 0
[now one resumes the common command set, taking care to include the two additional loopback
interfaces]:
router-4(config-router)# mpls traffic-eng router-id Loopback0
router-4(config-router)# mpls traffic-eng router-id Loopback1
router-4(config-router)# mpls traffic-eng router-id Loopback2
router-4(config-router)# exit

```

Create a virtual interface:

```

router-4(config)# interface Loopback0
router-4(config-if)# ip address 172.16.27.1 255.255.255.255
router-4(config-if)# exit

```

At the physical interface (ingress):

```

router-4(config)# interface pos2/1
router-4(config-if)# ip address 192.168.12.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

router-4(config)# interface pos2/2
router-4(config-if)# ip address 192.168.14.2 255.0.0.0
router-4(config-if)# mpls traffic-eng tunnels
router-4(config-if)# ip rsvp bandwidth 140000 140000 sub-pool 70000
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

```

## Configuring QoS Policy Propagation

On the tail device, one must configure a separate virtual loopback IP address for each class-of-service terminating here. The headend routers need these addresses to map traffic into the proper tunnels. In the current example, four tunnels terminate on the same tail device but they represent only two service classes, so only two additional loopback addresses are needed:

Create two virtual interfaces:

```

router-4(config)# interface Loopback1
router-4(config-if)# ip address 172.16.29.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit
router-4(config)# interface Loopback2
router-4(config-if)# ip address 172.16.30.1 255.255.255.255
[and if using IS-IS instead of OSPF]:
router-4(config-if)# ip router isis
[and in all cases]:
router-4(config-if)# exit

```

At the device level, configure BGP to send the community to each tunnel head:

```
router-4(config)# ip bgp-community new-format
router-4(config)# router bgp 2
router-4(config-router)# neighbor 172.16.23.1 send-community
router-4(config-router)# neighbor 172.16.22.1 send-community
router-4(config-router)# exit
```

# Additional References

The following sections provide references related to MPLS Traffic Engineering—DiffServ Aware.

## Related Documents

Related Topic	Document Title
Configuring OSPF	“Configuring OSPF” section in the <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a> , Release 12.4
OSPF commands	“OSPF Commands” section in the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4T
Configuring integrated IS-IS	“Configuring Integrated IS-IS” section in the <a href="#">Cisco IOS IP Routing Protocols Configuration Guide</a> , Release 12.4
Integrated IS-IS commands	“Integrated IS-IS Commands” section in the <a href="#">Cisco IOS IP Routing Protocols Command Reference</a> , Release 12.4T
Configuring RSVP	“Configuring RSVP” section in the <a href="#">Cisco IOS Quality of Service Solutions Configuration Guide</a> , Release 12.4
IP RSVP commands	<a href="#">Cisco IOS Quality of Service Solutions Command Reference</a> , Release 12.4T
Configuring QoS	<a href="#">Cisco IOS Quality of Service Solutions Configuration Guide</a> , Release 12.4
QoS commands	<a href="#">Cisco IOS Quality of Service Solutions Command Reference</a> , Release 12.4T
MPLS traffic engineering	<ul style="list-style-type: none"> <li>• <a href="#">MPLS Traffic Engineering and Enhancements</a>, Cisco IOS Release 12.1(3)T</li> <li>• “Multiprotocol Label Switching” chapter in the <a href="#">Cisco IOS Switching Services Configuration Guide</a>, Release 12.1</li> <li>• <a href="#">Cisco IOS Switching Command Reference</a>, Release 12.4T</li> </ul>

## Standards

Standard	Title
None	—

## MIBs

MIB	MIBs Link
None	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFC	Title
RFC 4124	<i>Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering</i>
RFC 4125	<i>Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering</i>
RFC 4127	<i>Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering</i>

## Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

## Command Reference

This section documents modified commands only.

- [debug mpls traffic-eng link-management preemption](#)
- [interface](#)
- [ip cef](#)
- [ip router isis](#)
- [ip rsvp bandwidth](#)
- [is-type](#)
- [metric-style wide](#)
- [mpls traffic-eng](#)
- [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 (global configuration)**
- **mpls traffic-eng tunnels (interface configuration)**
- **net**
- **passive-interface**
- **router isis**
- **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**

# debug mpls traffic-eng link-management preemption

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

**debug mpls traffic-eng link-management preemption [detail]**

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

Syntax Description	<b>detail</b> (Optional) Prints detailed debugging information.
--------------------	---

Defaults	No default behavior or values
----------	-------------------------------

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

```
Router# 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
```

# interface

To configure an interface type and enter interface configuration mode, use the **interface** command in global configuration mode.

## Standard Syntax

**interface** *type number [name-tag]*

## Analysis Module Network Module

**interface analysis-module** *slot/unit*

## Content Engine Network Module

**interface content-engine** *slot/unit*

## Cisco 830 Series

**interface** *type [number]*

## Cisco 2600 Series

**interface** *type slot/{port-adapter | port.subinterface-number}*

## Cisco 2600 Series on Voice Interfaces

**interface** *type slot/voice-module-slot/voice-interface-slot*

## Cisco 3600 Series

**interface** *type slot/{port | port.subinterface-number}*

## Cisco 3600 Series on Voice Interfaces

**interface** *type slot/voice-module-slot/voice-interface-slot*

## Cisco 7100 Series

**interface** *type slot/{port-adapter | port.subinterface-number}*

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

**interface** *type slot/port*

## Cisco 7200 VXR Router Used as a Router Shelf in a Cisco AS5800 Universal Access Server

**interface** *type router-shelf/slot/port*

## Cisco 7500 Series with Channelized T1 or E1

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



## Cisco 7500 Series with Ports on VIP Cards

```
interface type slot/port-adapter/port
```

To configure a subinterface, use this form of the **interface** global configuration command.

## Cisco 7200 Series

```
interface type slot/port.subinterface-number [multipoint | point-to-point]
```

## Cisco 7500 Series

```
interface type slot/port-adapter.subinterface-number [multipoint | point-to-point]
```

## Cisco 7500 Series with Ports on VIP Cards

```
interface type slot/port-adapter/port.subinterface-number [multipoint | point-to-point]
```

## Cisco 12000 Series

```
interface type slot{port-adapter | port.subinterface-number}
```

## Shared Port Adapters

```
interface type slot/subslot/port[.subinterface-number]
```

Syntax Description		
<i>type</i>		Type of interface to be configured. See <a href="#">Table 1</a> .
<i>number</i>		Port, connector, or interface card number. On Cisco 830 series routers, <i>number</i> specifies the ethernet interface number. On Cisco 4700 series routers, specifies the network interface module (NIM) or network processor module (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>name-tag</i>		(Optional) Specifies the logic name to identify the server configuration so that multiple server configurations can be entered.  This optional argument is for use with the Redundant Link Manager (RLM) feature.
<i>slot</i>		Chassis slot number.  Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
<i>/voice-module-slot</i>		Voice module slot number.  Refer to the “Cisco 3700 Series Routers Voice Interface Numbering” section of the “Understanding Interface Numbering and Cisco IOS Basics” chapter in the platform-specific SPA software configuration guide.

<i>/voice-interface-slot</i>	Voice interface slot number.  Refer to the “Cisco 3700 Series Routers Voice Interface Numbering” section of the “Understanding Interface Numbering and Cisco IOS Basics” chapter in the platform-specific SPA software configuration guide.
<i>/subslot</i>	Secondary slot number on a SIP where a SPA is installed.  Refer to the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on a SPA” topic in the platform-specific SPA software configuration guide for subslot information.
<i>/unit</i>	Number of the daughter card on the network module. For analysis module and content engine (CE) network modules, always use 0.
<i>/port</i>	Port or interface number.  Refer to the appropriate hardware manual for port information. For SPAs, refer to the corresponding “Specifying the Interface Address on a SPA” topics in the platform-specific SPA software configuration guide.
<i>router-shelf</i>	Router shelf number in a Cisco AS5800 universal access server. Refer to the appropriate hardware manual for router shelf information.
<i>:channel-group</i>	Channel group number. Cisco 7500 series routers specify the channel group number in the range of 0 to 4 defined with the <b>channel-group</b> controller configuration command.
<i>/port-adapter</i>	Port adapter number. Refer to the appropriate hardware manual for information about port adapter compatibility.
<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.

**Command Default** No interface types are configured.

**Command Modes** Global configuration



**Note**

To use this command with the RLM feature, you must be in interface configuration mode.

#### Command History

Release	Modification
10.0	This command was introduced for the Cisco 7000 series routers.
11.0	This command was implemented on the Cisco 4000 series routers.
12.0(3)T	The optional <i>name-tag</i> argument was added for the RLM feature.
12.2(13)T	The <b>content-engine</b> keyword was added.
12.2(15)T	The <b>lex</b> keyword was removed because the LAN Extension feature is no longer available in Cisco IOS software.

Release	Modification
12.3(7)T	The <b>analysis-module</b> keyword was added.
12.2(20)S2	This command was implemented for SPAs on the Cisco 7304 router.
12.2(18)SXE	This command was implemented for SPAs on the Cisco 7600 series routers and Catalyst 6500 series switches.
12.0(31)S	This command was implemented for SPAs on the Cisco 12000 series routers.
12.2(18)SXF	The <b>tengigabitethernet</b> keyword was added for support of the 10 Gigabit Ethernet interface type.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

### Usage Guidelines

This command does not have a **no** form.

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

[Table 1](#) displays the keywords that represent the types of interfaces that can be configured with the **interface** command. Replace the *type* argument with the appropriate keyword from the table.

**Table 1**      *Interface Type Keywords*

Keyword	Interface Type
<b>analysis-module</b>	Analysis module interface. The analysis module interface is a Fast Ethernet interface on the router that connects to the internal interface on the Network Analysis Module (NAM). This interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters.
<b>async</b>	Port line used as an asynchronous interface.
<b>atm</b>	ATM interface.
<b>bri</b>	ISDN 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>content-engine</b>	Content engine (CE) network module interface. The CE network module interface cannot be configured for subinterfaces or for speed, duplex mode, and similar parameters. See the command-line interface (CLI) help for a list of valid parameters. The <b>content-engine</b> keyword was formerly documented as the <b>interface content-engine</b> command.
<b>dialer</b>	Dialer interface.
<b>ethernet</b>	Ethernet IEEE 802.3 interface.
<b>fastethernet</b>	100-Mbps Ethernet interface. The <b>fastethernet</b> keyword was formerly documented as the <b>interface fastethernet</b> command.
<b>fddi</b>	FDDI interface.
<b>gigabitethernet</b>	1000-Mbps Ethernet interface. The <b>gigabitethernet</b> keyword was formerly documented as the <b>interface gigabitethernet</b> command.

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

Keyword	Interface Type
<b>group-async</b>	Master asynchronous interface. The <b>group-async</b> keyword was formerly documented as the <b>interface group-async</b> command.
<b>hssi</b>	High-Speed Serial Interface (HSSI).
<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>number</i> argument is the number of the loopback interface that you want to create or configure. There is no limit on the number of loopback interfaces that you can create.
<b>null</b>	Null interface.
<b>port-channel</b>	Port channel interface. The <b>port-channel</b> keyword was formerly documented as the <b>interface port-channel</b> command.
<b>pos</b>	Packet OC-3 interface on the Packet-over-SONET (POS) interface processor. The <b>pos</b> keyword was formerly documented as the <b>interface pos</b> command.
<b>sdcc</b>	Section data communications channel interface.
<b>serial</b>	Serial interface.
<b>switch</b>	Switch interface.
<b>tengigabitethernet</b>	10 Gigabit Ethernet interface.
<b>tokenring</b>	Token Ring interface.
<b>tunnel</b>	Tunnel interface; a virtual interface. The <i>number</i> argument is the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces that you can create.
<b>vg-anylan</b>	100VG-AnyLAN port adapter. The <b>vg-anylan</b> keyword was formerly documented as the <b>interface vg-anylan</b> command.

**Using the analysis-module Keyword**

The analysis module interface is used to access the NAM console for the initial configuration. After the NAM IP parameters are configured, the analysis module interface is typically used only during NAM software upgrades and while troubleshooting if the NAM Traffic Analyzer is inaccessible.

Visible only to the Cisco IOS software on the router, the analysis module interface is an internal Fast Ethernet interface on the router that connects to the internal NAM interface. The analysis module interface is connected to the router's Peripheral Component Interconnect (PCI) backplane, and all configuration and management of the analysis module interface must be performed from the Cisco IOS CLI.

**Using the group-async Keyword**

Using the **group-async** keyword, you create a single asynchronous interface with which other interfaces are associated as members using the **group-range** command. This one-to-many configuration allows you to configure all associated member interfaces by entering one command on the group master interface, rather than entering this command on each individual interface. You can create multiple group masters on a device; however, each member interface can be associated only with one group.

### Using the port-channel Keyword

The Fast EtherChannel feature allows multiple Fast Ethernet point-to-point links to be bundled into one logical link to provide bidirectional bandwidth of up to 800 Mbps. You can configure the port-channel interface as you would any Fast Ethernet interface.

After you create a port-channel interface, you assign Fast Ethernet interfaces (up to four) to it. For information on how to assign a Fast Ethernet interface to a port-channel interface, refer to the **channel-group** command in the interface configuration mode.



#### Caution

The port-channel interface is the routed interface. Do not enable Layer 3 addresses on the physical Fast Ethernet interfaces. Do not assign bridge groups on the physical Fast Ethernet interfaces because doing so creates loops. Also, you must disable spanning tree.



#### Caution

With Release 11.1(20)CC, the Fast EtherChannel supports Cisco Express Forwarding (CEF) and distributed Cisco Express Forwarding (dCEF). We recommend that you clear all explicit **ip route-cache distributed** commands from the Fast Ethernet interfaces before enabling dCEF on the port-channel interface. Clearing the route cache gives the port-channel interface proper control of its physical Fast Ethernet links. When you enable CEF/dCEF globally, all interfaces that support CEF/dCEF are enabled. When CEF/dCEF is enabled on the port-channel interface, it is automatically enabled on each of the Fast Ethernet interfaces in the channel group. However, if you have previously disabled CEF/dCEF on the Fast Ethernet interface, CEF/dCEF is not automatically enabled. In this case, you must enable CEF/dCEF on the Fast Ethernet interface.

As you work with the **port-channel** keyword, consider the following points:

- Currently, if you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the port-channel interface and not on the physical Fast Ethernet interface.
- If you do not assign a static MAC address on the port-channel interface, the Cisco IOS software automatically assigns a MAC address. If you assign a static MAC address and then later remove it, Cisco IOS software automatically assigns a MAC address.

### Using the vg-anylan Keyword

The 100VG-AnyLAN port adapter provides a single interface port that is compatible with and specified by IEEE 802.12. The 100VG-AnyLAN port adapter provides 100 Mbps over Category 3 or Category 5 unshielded twisted-pair (UTP) cable with RJ-45 terminators, and supports IEEE 802.3 Ethernet packets.

You configure the 100VG-AnyLAN port adapter as you would any Ethernet or Fast Ethernet interface. The 100VG-AnyLAN port adapter can be monitored with the IEEE 802.12 Interface MIB.

## Examples

### Serial Interface with PPP Encapsulation Example

The following example shows how to configure serial interface 0 with PPP encapsulation:

```
Router(config)# interface serial 0
Router(config-if)# encapsulation ppp
```

### Loopback Interface Example

The following example shows how to enable 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.

```
Router(config)# interface loopback 0
Router(config-if)# ip address 10.108.1.1 255.255.255.0
```

### Ethernet Port on Ethernet Interface Processor on Cisco 7500 Series Router Example

The following example shows how to configure Ethernet port 4 on the Ethernet Interface Processor (EIP) in slot 2 on the Cisco 7500 series router:

```
Router(config)# interface ethernet 2/4
```

### Token Ring Interface Processor Example

The following example shows how to configure the Token Ring interface processor in slot 1 on port 0 of a Cisco 7500 series router:

```
Router(config)# interface tokenring 1/0
```

### Analysis Module Interface with NAM Router Example

The following example configures an analysis module interface when the NAM router is in router slot 1:

```
Router(config)# interface analysis-module 1/0
```

### Content Engine Network Module Interface Example

The following example configures an interface for a content engine network module in slot 1:

```
Router(config)# interface content-engine 1/0
```

### Ethernet Interface on Cisco 830 Router Example

The following example configures a new interface **ethernet2** on the LAN or on the WAN side of the Cisco 830 Series router.

```
c837#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
c837(config)#interface ethernet 2
```

### Fast Ethernet Interface on Cisco 2600 Router Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 2600 series router:

```
Router(config)# interface fastethernet0/0
or
Router(config)# interface fastethernet0/0.1
```

### Fast Ethernet Interface on Cisco 3600 Router Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 3600 series router:

```
Router(config)# interface fastethernet0/0
or
Router(config)# interface fastethernet0/0.1
```

### Fast Ethernet Interface with ARPA Encapsulation on Cisco 4700 Router Example

The following example shows how to configure Fast Ethernet interface 0 for standard ARPA encapsulation (the default setting) on a Cisco 4700 series router:

```
Router(config)# interface fastethernet 0
```

### Gigabit Ethernet Interface Example

The following example shows how to configure the Gigabit Ethernet interface for slot 0, port 0:

```
Router(config)# interface gigabitethernet 0/0
```

### Asynchronous Group Master Interface Example

The following example shows how to define asynchronous group master interface 0:

```
Router(config)# interface group-async 0
```

### Port Channel Interface Example

The following example shows how to create a port-channel interface with a channel group number of 1 and adds two Fast Ethernet interfaces to port-channel 1:

```
Router(config)# interface port-channel 1
Router(config-if)# ip address 10.1.1.10 255.255.255.0
Router(config-if)# exit
Router(config)# interface fastethernet 1/0/0
Router(config-if)# channel-group 1
Router(config-if)# exit
Router(config)# interface fastethernet 4/0/0
Router(config-if)# channel-group 1
```

### Packet over SONET Interface Example

The following example shows how to specify the single Packet OC-3 interface on port 0 of the POS OC-3 port adapter in slot 2:

```
Router(config)# interface pos 2/0
```

### 100VG-AnyLAN Interface Example

The following example shows how to specify the 100VG-AnyLAN port adapter in the first port adapter in slot 1:

```
Router(config)# interface vg-anylan 1/0/0
```

### Fast Ethernet Interface on Cisco 7100 Router Example

The following example shows how to configure Fast Ethernet interface 0 on a Cisco 7100 series router:

```
Router(config)# interface fastethernet0/0
or
Router(config)# interface fastethernet0/0.1
```

### Fast Ethernet Interface on Cisco 12000 Router Example

The following example shows how to configure Fast Ethernet interface 6 on a Cisco 12000 series router:

```
Router(config)# interface fastethernet6/0
or
Router(config)# interface fastethernet6/0.1
```

### Partially Meshed Frame Relay Network Example

The following example shows how to configure a partially meshed Frame Relay network. In this example, subinterface serial 0.1 is configured as a multipoint subinterface with two associated Frame Relay permanent virtual connections (PVCs), and subinterface serial 0.2 is configured as a point-to-point subinterface.

```
Router(config)# interface serial 0
Router(config-if)# encapsulation frame-relay
Router(config-if)# exit
Router(config)# interface serial 0/0.1 multipoint
Router(config-if)# ip address 10.108.10.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 42 broadcast
Router(config-if)# frame-relay interface-dlci 53 broadcast
Router(config-if)# exit
Router(config)# interface serial 0/0.2 point-to-point
Router(config-if)# ip address 10.108.11.1 255.255.255.0
Router(config-if)# frame-relay interface-dlci 59 broadcast
```

### T1 Serial Interface Example

The following example shows how to configure circuit 0 of a T1 link for PPP encapsulation:

```
Router(config)# controller t1 4/1
Router(config-controller)# circuit 0 1
Router(config-controller)# exit
Router(config)# interface serial 4/1:0
Router(config-if)# ip address 10.108.13.1 255.255.255.0
Router(config-if)# encapsulation ppp
```

### SDCC Interface on a POS Shared Port Adapter Example

The following example configures the first interface (port 0) as a section data communications channel (SDCC) interface on a POS SPA, where the SPA is installed in the top subslot (0) of the MSC, and the MSC is installed in slot 4 of the Cisco 7304 router:

```
Router(config)# interface sdcc 4/3/0
Router(config-if)# ip address 10.1.9.2 255.255.255.0
Router(config-if)# logging event link-status
Router(config-if)# load-interval 30
Router(config-if)# no keepalive
Router(config-if)# no fair-queue
Router(config-if)# no cdp enable
```

### Shared Port Adapter Interface Example

The following example configures the second interface (port 1) on a 4-Port 10/100 Fast Ethernet SPA for standard ARPA encapsulation (the default setting), where the SPA is installed in the bottom subslot (1) of the MSC, and the MSC is installed in slot 2 of the Cisco 7304 router:

```
Router(config)# interface fastethernet 2/1/1
```

#### Related Commands

Command	Description
<b>channel-group</b>	Defines the timeslots that belong to each T1 or E1 circuit.
<b>channel-group (Fast EtherChannel)</b>	Assigns a Fast Ethernet interface to a Fast EtherChannel group.
<b>clear interface</b>	Resets the hardware logic on an interface.
<b>controller</b>	Configures an E1, J1, T1, or T3 controller and enters controller configuration mode.



Command	Description
<b>group-range</b>	Creates a list of asynchronous interfaces that are associated with a group interface on the same device.
<b>mac-address</b>	Sets the MAC layer address.
<b>ppp</b>	Starts an asynchronous connection using PPP.
<b>show controllers content-engine</b>	Displays controller information for CE network modules.
<b>show interfaces</b>	Displays information about interfaces.
<b>show interfaces content-engine</b>	Displays basic interface configuration information for a CE network module.
<b>shutdown (RLM)</b>	Shuts down all of the links under the RLM group.
<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** command in global configuration mode. To disable CEF, use the **no** form of this command.

**ip cef [distributed]**

**no ip cef [distributed]**

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

<b>Defaults</b>	<p>CEF is disabled by default, excluding these platforms:</p> <ul style="list-style-type: none"> <li>CEF is enabled on the Cisco 7100 series router.</li> <li>CEF is enabled on the Cisco 7200 series router.</li> <li>CEF is enabled on the Cisco 7500 series Internet router.</li> <li>Distributed CEF is enabled on the Cisco 6500 series router</li> <li>Distributed CEF is enabled on the Cisco 12000 series Internet router.</li> </ul>
-----------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	11.1 CC	This command was introduced.
	12.2	The default for Cisco 7200 series routers was changed from disabled to enabled.
	12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T and implemented on the following platforms: Cisco IAD2420 series, Cisco 2600 series, Cisco 3620 routers, Cisco 3640 routers, Cisco 3660 routers, Cisco 3700 series routers, and Cisco MC3810 multiservice access concentrators.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Usage Guidelines</b>	<p>The <b>ip cef</b> command is not available on the Cisco 12000 series because that router series operates only in dCEF mode.</p> <p>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.</p> <p>If you enable CEF and then create an access list that uses the <b>log</b> keyword, the packets that match the access list are not CEF switched. They are fast switched. Logging disables CEF.</p>
-------------------------	---

## Examples

The following example shows how to enable standard CEF operation:

```
Router(config)# ip cef
```

The following example shows how to enable dCEF operation:

```
Router(config)# ip cef distributed
```

## Related Commands

Command	Description
<b>ip route-cache</b>	Controls the use of high-speed switching caches for IP routing.
<b>ip cef accounting</b>	Enables CEF network accounting.
<b>ip cef load-sharing algorithm</b>	Selects a CEF load balancing algorithm.
<b>ip cef table adjacency-prefix override</b>	Enables CEF adjacency prefixes to override static host glean routes.
<b>ip cef table consistency-check</b>	Enables CEF table consistency checker types and parameters.
<b>ip cef table event-log</b>	Controls CEF table event-log characteristics.
<b>ip cef table resolution-timer</b>	Changes CEF background resolution timer.

# ip router isis

To configure an Intermediate System-to-Intermediate System (IS-IS) routing process for IP on an interface and to attach an area designator to the routing process, use the **ip router isis** command in interface configuration mode. To disable IS-IS for IP, use the **no** form of the command.

**ip router isis** *area-tag*

**no ip router isis** *area-tag*

Syntax Description	<table> <tr> <td data-bbox="342 575 600 611"><i>area-tag</i></td><td data-bbox="600 575 1485 865"> <p>Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.</p> <p>Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.</p> <p><b>Note</b> Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.</p> </td></tr> </table>	<i>area-tag</i>	<p>Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.</p> <p>Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.</p> <p><b>Note</b> Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.</p>
<i>area-tag</i>	<p>Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.</p> <p>Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.</p> <p><b>Note</b> Each area in a multiarea configuration should have a nonnull area tag to facilitate identification of the area.</p>		

Defaults	No routing processes are specified.
----------	-------------------------------------

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(5)T	Multiarea functionality was added, changing the way the <i>tag</i> argument (now <i>area-tag</i> ) is used.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines	<p>Before the IS-IS routing process is useful, a network entity title (NET) must be assigned with the <b>net</b> command and some interfaces must have IS-IS enabled.</p> <p>If you have IS-IS running and at least one International Organization for Standardization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.</p> <p>You can configure only one process to perform Level 2 (interarea) routing. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1. You can configure this process to perform intra-area (Level 1) routing at the same time. You can configure up to</p>
------------------	--

29 additional processes as Level 1-only processes. Use the **is-type** command to remove Level 2 routing from a router instance. You can then use the **is-type** command to enable Level 2 routing on some other IS-IS router instance.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

## Examples

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows an IS-IS configuration with two Level 1 areas and one Level 1-2 area:

```
ip routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
1
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02

.
.
.

! Defaults to "is-type level-1-2"
router isis BB
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

**Related Commands**

Command	Description
<b>is-type</b>	Configures the routing level for an IS-IS routing process.
<b>net</b>	Configures an IS-IS NET for a CLNS routing process.
<b>router isis</b>	Enables the IS-IS routing protocol.

# ip rsvp bandwidth

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

**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>	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows. The range is from 1 to 10,000,000.
	<i>single-flow-kbps</i>	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10,000,000. This value is ignored by the Diff-Serv-aware MPLS Traffic Engineering feature available with Cisco IOS Release 12.2(4)T.
	<b>sub-pool</b> <i>kbps</i>	(Optional) 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 the <i>interface-kbps</i> argument.

## Defaults

RSVP is disabled by default.

If the **ip rsvp bandwidth** command is entered but no bandwidth values are supplied (for example, **ip rsvp bandwidth** is entered followed by pressing the Enter key), a default bandwidth value (that is, 75% of the link bandwidth) is assumed for both the *interface-kbps* and *single-flow-kbps* arguments.

## Command Modes

Interface configuration

## Command History

Release	Modification
11.2	This command was introduced.
12.0(11)ST	The <b>sub-pool</b> keyword was added.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T. This command was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

RSVP cannot be configured with 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 queueing must be enabled first.

**Examples**

The following example shows a T1 (1536 kbps) link configured to permit RSVP reservation of up to 1158 kbps, but no more than 100 kbps for any given flow on serial interface 0. Fair queueing is configured with 15 reservable queues to support those reserved flows, should they be required.

```
Router(config)# interface serial 0
Router(config-if)# fair-queue 64 256 15
Router(config-if)# ip rsvp bandwidth 1158 100
```

**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.



# is-type

To configure the routing level for an instance of the Intermediate System-to-Intermediate System (IS-IS) routing process, use the **is-type** command in router configuration mode. To reset the default value, use the **no** form of this command.

**is-type** [**level-1** | **level-1-2** | **level-2-only**]

**no is-type** [**level-1** | **level-1-2** | **level-2-only**]

Syntax Description		
<b>level-1</b>	(Optional) Router performs only Level 1 (intra-area) routing. This router learns only about destinations inside its area. Level 2 (interarea) routing is performed by the closest Level 1-2 router.	
<b>level-1-2</b>	(Optional) Router performs both Level 1 and Level 2 routing. This router runs two instances of the routing process. It has one link-state packet database (LSDB) for destinations inside the area (Level 1 routing) and runs a shortest path first (SPF) calculation to discover the area topology. It also has another LSDB with link-state packets (LSPs) of all other backbone (Level 2) routers, and runs another SPF calculation to discover the topology of the backbone, and the existence of all other areas.	
<b>level-2-only</b>	(Optional) Routing process acts as a Level 2 (interarea) router only. This router is part of the backbone, and does not communicate with Level 1-only routers in its own area.	

## Defaults

In conventional IS-IS configurations, the router acts as both a Level 1 (intra-area) and a Level 2 (interarea) router.

In multiarea IS-IS configurations, the first instance of the IS-IS routing process configured is by default a Level 1-2 (intra-area and interarea) router. The remaining instances of the IS-IS process configured by default are Level 1 routers.

## Command Modes

Router configuration

## Command History

Release	Modification
10.3	This command was introduced.
12.0(5)T	This command was modified to include multiarea IS-IS routing.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

We highly recommend that you configure the type of IS-IS routing process. If you are configuring multiarea IS-IS, you *must* configure the type of the router, or allow it to be configured by default. By default, the first instance of the IS-IS routing process that you configure using the **router isis** command is a Level 1-2 router.

If only one area is in the network, there is no need to run both Level 1 and Level 2 routing algorithms. If IS-IS is used for Connectionless Network Service (CLNS) routing (and there is only one area), Level 1 only must be used everywhere. If IS-IS is used for IP routing only (and there is only one area), you can run Level 2 only everywhere. Areas you add after the Level 1-2 area exists are by default Level 1 areas.

If the router instance has been configured for Level 1-2 (the default for the first instance of the IS-IS routing process in a Cisco device), you can remove Level 2 (interarea) routing for the area using the **is-type** command. You can also use the **is-type** command to configure Level 2 routing for an area, but it must be the only instance of the IS-IS routing process configured for Level 2 on the Cisco device.

---

## Examples

The following example specifies an area router:

```
router isis
 is-type level-2-only
```

---

## Related Commands

Command	Description
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process.
<b>show clns neighbor areas</b>	Displays information about IS-IS neighbors and the areas to which they belong.

# metric-style wide

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

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

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

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

**Defaults** The Multiprotocol Label Switching (MPLS) traffic engineering image generates only old-style TLVs. To do MPLS traffic engineering, a router must generate new-style TLVs that have wider metric fields.

**Command Modes** Router configuration

Command History	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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




## Note

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

**Examples** The following example shows how to configure a router to generate and accept only new-style TLVs on level 1:

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

 metric-style wide

Related Commands	Command	Description
	<b>metric-style narrow</b>	Configures a router to generate and accept old-style TLVs.
	<b>metric-style transition</b>	Configures a router to generate and accept both old-style and new-style TLVs.

# mpls traffic-eng

To configure a router running Intermediate System-to-Intermediate System (IS-IS) so that it floods Multiprotocol Label Switching (MPLS) traffic engineering (TE) link information into the indicated IS-IS level, use the **mpls traffic-eng** command in router configuration mode. To disable the flooding of MPLS TE link information into the indicated IS-IS level, use the **no** form of this command.

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

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

Syntax Description	<b>level-1</b>	Floods MPLS TE link information into IS-IS level 1.
	<b>level-2</b>	Floods MPLS TE link information into IS-IS level 2.
Defaults	Flooding is disabled.	
Command Modes	Router configuration	
Command History	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Usage Guidelines	This command, which is part of the routing protocol tree, causes link resource information (such as available bandwidth) for appropriately configured links to be flooded in the IS-IS link-state database.	
Examples	<p>The following example shows how to configure MPLS TE link information flooding for IS-IS level 1:</p> <pre>Router(config-router)# mpls traffic-eng level-1</pre>	
Related Commands	<b>Command</b>	<b>Description</b>
	<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.

# mpls traffic-eng administrative-weight

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

**mpls traffic-eng administrative-weight** *weight*

**no mpls traffic-eng administrative-weight**

Syntax Description	<i>weight</i> Cost of the link.	
Defaults	IGP cost of the link.	
Command Modes	Interface configuration	
Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Examples	<p>The following example shows how to override the IGP cost of the link and set the cost to 20:</p> <pre>Router(config-if)# mpls traffic-eng administrative-weight 20</pre>	
Related Commands	Command	Description
	<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 Open Shortest Path First (OSPF) Multiprotocol Label Switching (MPLS) so that it floods traffic engineering for the indicated OSPF area, use the **mpls traffic-eng area** command in router configuration mode. To disable flooding of traffic engineering for the indicated OSPF area, use the **no** form of this command.

**mpls traffic-eng area** *number*

**no mpls traffic-eng area** *number*

Syntax Description	<i>number</i>	The OSPF area on which MPLS traffic engineering is enabled.
Defaults	Flooding is disabled.	
Command Modes	Router configuration	
Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Usage Guidelines	This command is in the routing protocol configuration tree and is supported for both OSPF and IS-IS. The command affects the operation of MPLS traffic engineering only if MPLS traffic engineering is enabled for that routing protocol instance. Currently, only a single level can be enabled for traffic engineering.	
Examples	<p>The following example shows how to configure a router running OSPF MPLS to flood traffic engineering for OSPF 0:</p> <pre>Router(config-router)# mpls traffic-eng area 0</pre>	
Related Commands	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** command in interface configuration mode. To disable the user-specified attribute flags for the interface, use the **no** form of this command.

**mpls traffic-eng attribute-flags** *attributes*

**no mpls traffic-eng attribute-flags**

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

Defaults	0x0
----------	-----

Command Modes	Interface configuration
---------------	-------------------------

Command History	<table> <tr> <th data-bbox="342 1022 617 1066">Release</th><th data-bbox="617 1022 1487 1066">Modification</th></tr> <tr> <td data-bbox="342 1066 617 1110">12.0(5)S</td><td data-bbox="617 1066 1487 1110">This command was introduced.</td></tr> <tr> <td data-bbox="342 1110 617 1146">12.2(28)SB</td><td data-bbox="617 1110 1487 1146">This command was integrated into Cisco IOS Release 12.2(28)SB.</td></tr> </table>	Release	Modification	12.0(5)S	This command was introduced.	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Release	Modification						
12.0(5)S	This command was introduced.						
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.						

Usage Guidelines	<p>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.</p> <p>The interface is flooded globally so that it can be used as a tunnel head-end path selection criterion.</p>
------------------	---

Examples	<p>The following example shows how to set the attribute flags to 0x0101:</p> <pre>Router(config-if)# mpls traffic-eng attribute-flags 0x0101</pre>
----------	--

Related Commands	<table> <tr> <th data-bbox="342 1560 836 1604">Command</th><th data-bbox="836 1560 1487 1604">Description</th></tr> <tr> <td data-bbox="342 1604 836 1648"><b>mpls traffic-eng administrative-weight</b></td><td data-bbox="836 1604 1487 1648">Overrides the IGP administrative weight of the link.</td></tr> <tr> <td data-bbox="342 1648 836 1745"><b>tunnel mpls traffic-eng affinity</b></td><td data-bbox="836 1648 1487 1745">Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.</td></tr> </table>	Command	Description	<b>mpls traffic-eng administrative-weight</b>	Overrides the IGP administrative weight of the link.	<b>tunnel mpls traffic-eng affinity</b>	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.
Command	Description						
<b>mpls traffic-eng administrative-weight</b>	Overrides the IGP administrative weight of the link.						
<b>tunnel mpls traffic-eng affinity</b>	Configures affinity (the properties that the tunnel requires in its links) for an MPLS traffic engineering tunnel.						



# mpls traffic-eng backup-path tunnel

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

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

<b>Syntax Description</b>	<i>interface</i>	String that identifies the tunnel interface being created and configured.
---------------------------	------------------	---

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

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

<b>Command History</b>	Release	Modification
	12.0(8)ST	This command was introduced.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SX.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Examples</b>	The following example shows you how to specify the traffic engineering backup tunnel with the identifier 1000:
-----------------	--

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

<b>Related Commands</b>	Command	Description
	<b>show mpls traffic-eng fast-reroute database</b>	Displays information about existing Fast Reroute configurations.
	<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 reserved bandwidth thresholds for a link, use the **mpls traffic-eng flooding thresholds** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**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 reserved bandwidth.
<b>up</b>	Sets the thresholds for increased reserved bandwidth.
<i>percent [percent]</i>	Bandwidth threshold level. For the <b>down</b> keyword, valid values are from 0 through 99. For the <b>up</b> keyword, valid values are 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.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

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

## Examples

The following example shows how to set the reserved bandwidth of the link for decreased (down) and for increased (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 timers periodic-flooding</b>	Sets the length of the interval used for periodic flooding.
	<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.

## mpls traffic-eng link timers bandwidth-hold

To set the length of time that bandwidth is held for a Resource Reservation Protocol (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 in global configuration mode.

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

Syntax Description	<i>hold-time</i>	Sets the length of time that bandwidth can be held. The range is from 1 to 300 seconds.
Defaults	15 seconds	
Command Modes	Global configuration	
Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Examples	<p>The following example sets the length of time that bandwidth is held to 10 seconds.</p> <pre>Router(config)# mpls traffic-eng link-management timers bandwidth-hold 10</pre>	
Related Commands	Command	Description
	<b>show mpls traffic-eng link-management bandwidth-allocation</b>	Displays 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 in global configuration mode.

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

Syntax Description	<i>interval</i>  Length of interval used for periodic flooding (in seconds). The range is from 0 to 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	180 seconds							
Command Modes	Global configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(5)S</td><td>This command was introduced.</td></tr><tr><td>12.2(28)SB</td><td>This command was integrated into Cisco IOS Release 12.2(28)SB</td></tr></table>		Release	Modification	12.0(5)S	This command was introduced.	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB
Release	Modification							
12.0(5)S	This command was introduced.							
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB							
Usage Guidelines	<p>Use this command to set the interval for periodic flooding of traffic engineering (TE) topology information.</p> <p>Changes in the Multiprotocol Label Switching (MPLS) TE topology database are flooded by the link state Interior Gateway Protocol (IGP). Some changes, such as those to link status (up/down) or configured parameters, trigger immediate flooding. Other changes are considered less urgent and are flooded periodically. For example, changes to the amount of link bandwidth allocated to TE tunnels are flooded periodically unless the change causes the bandwidth to cross a configurable threshold.</p>							
Examples	<p>The following example sets the interval length for periodic flooding to advertise flooding changes to 120 seconds.</p> <pre>Router(config)# mpls traffic-eng timers periodic-flooding 120</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td><b>mpls traffic-eng flooding thresholds</b></td><td>Sets the reserved bandwidth thresholds of a link.</td></tr></table>		Command	Description	<b>mpls traffic-eng flooding thresholds</b>	Sets the reserved bandwidth thresholds of a link.		
Command	Description							
<b>mpls traffic-eng flooding thresholds</b>	Sets the reserved bandwidth thresholds of a link.							

# mpls traffic-eng reoptimize timers frequency

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

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

**no mpls traffic-eng reoptimize timers frequency**

<b>Syntax Description</b>	<i>seconds</i>	Sets the frequency of reoptimization (in seconds). A value of 0 disables reoptimization. The range of values is 0 to 604800 seconds (1 week)
---------------------------	----------------	--

<b>Defaults</b>	3600 seconds (1 hour)
-----------------	-----------------------

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

<b>Command History</b>	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Usage Guidelines</b>	A device with traffic engineering tunnels periodically examines tunnels with established LSPs to learn if better LSPs are available. If a better LSP seems to be available, the device attempts to signal the better LSP; if the signalling is successful, the device replaces the old, inferior LSP with the new, better LSP.
-------------------------	--



**Note**

If the **lockdown** keyword is specified with the **tunnel mpls traffic-eng path-option** command, then a reoptimize check is not done on the tunnel.

<b>Examples</b>	The following example shows how to set the reoptimization frequency to 1 day:  Router(config)# <b>mpls traffic-eng reoptimize timers frequency 86400</b>
-----------------	--

<b>Related Commands</b>	Command	Description
	<b>mpls traffic-eng reoptimize</b>	Reoptimizes all traffic engineering tunnels immediately.
	<b>tunnel mpls traffic-eng path-option</b>	Configures a path option for an MPLS traffic engineering 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** command in router configuration mode. To remove the traffic engineering router identifier, use the **no** form of this command.

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

**no mpls traffic-eng router-id**

Syntax Description	<i>interface-name</i> Interface whose primary IP address is the router's identifier.							
Defaults	No traffic engineering router identifier is specified.							
Command Modes	Router configuration							
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>12.0(5)S</td><td>This command was introduced.</td></tr><tr><td>12.2(28)SB</td><td>This command was integrated into Cisco IOS Release 12.2(28)SB.</td></tr></table>		Release	Modification	12.0(5)S	This command was introduced.	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
Release	Modification							
12.0(5)S	This command was introduced.							
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.							
Usage Guidelines	<p>This router identifier acts as a stable IP address for the traffic engineering configuration. This IP address is flooded to all nodes. For all traffic engineering tunnels originating at other nodes and ending at this node, you must set the tunnel destination to the traffic engineering router identifier of the destination node, because that is the address that the traffic engineering topology database at the tunnel head uses for its path calculation.</p>							
Examples	<p>The following example shows how to specify the traffic engineering router identifier as the IP address associated with interface Loopback0:</p> <pre>Router(config-router)# mpls traffic-eng router-id Loopback0</pre>							
Related Commands	<table><tr><th>Command</th><th>Description</th></tr><tr><td><b>mpls atm control-vc</b></td><td>Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.</td></tr></table>		Command	Description	<b>mpls atm control-vc</b>	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.		
Command	Description							
<b>mpls atm control-vc</b>	Turns on flooding of MPLS traffic engineering link information in the indicated IGP level/area.							

# mpls traffic-eng tunnels (global configuration)

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel signaling on a device, use the **mpls traffic-eng tunnels** command in global configuration mode. To disable MPLS traffic engineering tunnel signaling, use the **no** form of this command.

**mpls traffic-eng tunnels**

**no mpls traffic-eng tunnels**

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

**Defaults** The command is disabled.

**Command Modes** Global configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

**Examples** The following example shows how to turn on MPLS traffic engineering tunnel signaling:

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

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



# **mpls traffic-eng tunnels (interface configuration)**

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

**mpls traffic-eng tunnels**

**no mpls traffic-eng tunnels**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	The command is disabled on all interfaces.
-----------------	--

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

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

<b>Examples</b>	The following example shows how to enable MPLS traffic engineering on Ethernet interface 0/0:
-----------------	---

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

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

# net

To configure an Intermediate System-to-Intermediate System (IS-IS) network entity title (NET) for a Connectionless Network Service (CLNS) routing process, use the **net** command in router configuration mode. To remove a NET, use the **no** form of this command.

**net** *network-entity-title*

**no net** *network-entity-title*

<b>Syntax Description</b>	<i>network-entity-title</i>	NET that specifies the area address and the system ID for a CLNS routing process. This argument can be either an address or a name.
---------------------------	-----------------------------	---

<b>Defaults</b>	No NET is configured and the CLNS process will not start. A NET is mandatory.
-----------------	---

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

<b>Command History</b>	Release	Modification
	10.0	This command was introduced.
	12.0(5)T	This command was modified to include multiarea IS-IS routing.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Usage Guidelines</b>	Under most circumstances, one and only one NET must be configured.
	A NET is a network service access point (NSAP) where the last byte is always zero. On a Cisco router running IS-IS, a NET can be 8 to 20 bytes. The last byte is always the n-selector and must be zero.
	The six bytes directly in front of the n-selector are the system ID. The system ID length is a fixed size and cannot be changed. The system ID must be unique throughout each area (Level 1) and throughout the backbone (Level 2).
	All bytes in front of the system ID are the area ID.
	Even when IS-IS is used to perform IP routing only (no CLNS routing enabled), a NET must still be configured to define the router system ID and area ID.
	A maximum of three NETs per router are allowed. In rare circumstances, it is possible to configure two or three NETs. In such a case, the area this router is in will have three area addresses. There will still be only one area, but it will have an additional maximum of three area addresses.
	Configuring multiple NETs can be temporarily useful in the case of network reconfiguration where multiple areas are merged, or where one area is split into additional areas. Multiple area addresses enable you to renumber an area individually as needed.
	If you are configuring multiarea IS-IS, the area ID must be unique, but the system ID portion of the NET must be the same for all IS-IS routing process instances.

**Examples**

The following example configures a router with system ID 0000.0c11.1111.00 and area ID 47.0004.004d.0001:

```
router isis FIRST
 net 47.0004.004d.0001.0001.0c11.1111.00
```

The following example shows three IS-IS routing processes with three areas configured. Each area has a unique identifier, but the system ID is the same for all areas.

```
clns routing

.
.
.

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

.
.
.

router isis BB                                ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

**Related Commands**

Command	Description
<b>is-type</b>	Configures the routing level for an instance of the IS-IS routing process.
<b>router isis</b>	Enables the IS-IS routing protocol and specifies an IS-IS process.

# passive-interface

To disable sending routing updates on an interface, use the **passive-interface** command in router configuration mode. To reenable the sending of routing updates, use the **no** form of this command.

**passive-interface** [**default**] {*interface-type* *interface-number*}

**no passive-interface** *interface-type interface-number*

Syntax Description	<b>default</b>	(Optional) All interfaces become passive.
	<i>interface-type</i>	Interface type.
	<i>interface-number</i>	Interface number.

**Defaults** Routing updates are sent on the interface.

**Command Modes** Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	The <b>default</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines**

If you disable the sending of routing updates on an interface, the particular subnet will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

The **default** keyword sets all interfaces as passive by default. You can then configure individual interfaces where adjacencies are desired using the **no passive-interface** command. The **default** keyword is useful in Internet service provider (ISP) and large enterprise networks where many of the distribution routers have more than 200 interfaces.

For the Open Shortest Path First (OSPF) protocol, OSPF routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPF domain.

For the Intermediate System-to-Intermediate System (IS-IS) protocol, this command instructs IS-IS to advertise the IP addresses for the specified interface without actually running IS-IS on that interface. The **no** form of this command for IS-IS disables advertising IP addresses for the specified address.



**Note** For IS-IS you must keep at least one active interface and configure the interface with the **ip router isis** command.

Enhanced Interior Gateway Routing Protocol (EIGRP) is disabled on an interface that is configured as passive although it advertises the route.

---

**Examples**

The following example sends EIGRP updates to all interfaces on network 10.108.0.0 except Ethernet interface 1:

```
router eigrp 109
 network 10.108.0.0
 passive-interface ethernet 1
```

The following configuration enables IS-IS on Ethernet interface 1 and serial interface 0 and advertises the IP addresses of Ethernet interface 0 in its link-state protocol data units (PDUs):

```
router isis Finance
 passive-interface Ethernet 0
 interface Ethernet 1
 ip router isis Finance
 interface serial 0
 ip router isis Finance
```

The following example sets all interfaces as passive, then activates Ethernet interface 0:

```
router ospf 100
 passive-interface default
 no passive-interface ethernet0
 network 10.108.0.1 0.0.0.255 area 0
```

# router isis

To enable the Intermediate System-to-Intermediate System (IS-IS) routing protocol and to specify an IS-IS process, use the **router isis** command in global configuration mode. To disable IS-IS routing, use the **no** form of this command.

**router isis** *area-tag*

**no router isis** *area-tag*

## Syntax Description

<i>area-tag</i>	Meaningful name for a routing process. If it is not specified, a null tag is assumed and the process is referenced with a null tag. This name must be unique among all IP or Connectionless Network Service (CLNS) router processes for a given router.  Required for multiarea IS-IS configuration. Optional for conventional IS-IS configuration.
-----------------	---

## Defaults

This command is disabled by default.

## Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	Multiarea functionality was added, changing the way the <i>tag</i> argument (now <i>area-tag</i> ) is used.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

This command is used to enable routing for an area. An appropriate network entity title (NET) must be configured to specify the area address of the area and system ID of the router. Routing must be enabled on one or more interfaces before adjacencies may be established and dynamic routing is possible.

If you have IS-IS running and at least one International Standards Organization Interior Gateway Routing Protocol (ISO-IGRP) process, the IS-IS process and the ISO-IGRP process cannot both be configured without an area tag. The null tag can be used by only one process. If you run ISO-IGRP and IS-IS, a null tag can be used for IS-IS, but not for ISO-IGRP at the same time. However, each area in an IS-IS multiarea configuration should have a nonnull area tag to facilitate identification of the area.

You can configure only one IS-IS routing process to perform Level 2 (interarea) routing. You can configure this process to perform Level 1 (intra-area) routing at the same time. You can configure up to 29 additional processes as Level 1-only processes. If Level 2 routing is configured on any process, all additional processes are automatically configured as Level 1.

An interface cannot be part of more than one area, except in the case where the associated routing process is performing both Level 1 and Level 2 routing. On media such as WAN media where subinterfaces are supported, different subinterfaces could be configured for different areas.

If Level 2 routing is not desired for a given area, use the **is-type** command to remove Level 2. Level 2 routing can then be enabled on some other router instance.

Explicit redistribution between IS-IS instances is prohibited (prevented by the parser). In other words, you cannot issue a **redistribute isis area-tag** command in the context of another IS-IS router instance (**router isis area-tag**). Redistribution from any other routing protocol into a particular area is possible, and is configured per router instance, as in Cisco IOS software Release 12.0, using the **redistribute** and **route map** commands. By default, redistribution is into Level 2.

If multiple Level 1 areas are defined, the Target Address Resolution Protocol (TARP) behaves in the following way:

- The locally assigned target identifier gets the network service access point (NSAP) of the Level 2 area, if present.
- If only Level 1 areas are configured, the router uses the NSAP of the first active Level 1 area as shown in the configuration at the time of TARP configuration (“tarp run”). (Level 1 areas are sorted alphanumerically by tag name, with capital letters coming before lowercase letters. For example, AREA-1 precedes AREA-2, which precedes area-1.) Note that the target identifier NSAP could change following a reload if a new Level 1 area is added to the configuration after TARP is running.
- The router continues to process all Type 1 and 2 protocol data units (PDUs) that are for this router. Type 1 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are “propagated” (routed) to all interfaces in the *same* Level 1 area. (The same area is defined as the area configured on the input interface.)
- Type 2 PDUs are processed locally if the specified target identifier is in the local target identifier cache. If not, they are propagated via all interfaces (all Level 1 or Level 2 areas) with TARP enabled. If the source of the PDU is from a different area, the information is also added to the local target identifier cache. Type 2 PDUs are propagated via all static adjacencies.
- Type 4 PDUs (for changes originated locally) are propagated to all Level 1 and Level 2 areas (because internally they are treated as “Level 1-2”).
- Type 3 and 5 PDUs continue to be routed.
- Type 1 PDUs are propagated only via Level 1 static adjacencies if the static NSAP is in one of the Level 1 areas in this router.

After you enter the **router isis** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

## Examples

The following example configures IS-IS for IP routing, with system ID 0000.0000.0002 and area ID 01.0001, and enables IS-IS to form adjacencies on Ethernet interface 0 and serial interface 0. The IP prefix assigned to Ethernet interface 0 will be advertised to other IS-IS routers.

```
router isis tag1
 net 01.0001.0000.0000.0002
 is-type level-1
!
interface ethernet 0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
!
interface serial 0
 ip unnumbered ethernet0
 ip router isis
```

The following example starts IS-IS routing with the optional *area-tag* argument, where CISCO is the value for the *area-tag* argument:

```
router isis CISCO
```

The following example specifies IS-IS as an IP routing protocol for a process named Finance, and specifies that the Finance process will be routed on Ethernet interface 0 and serial interface 0:

```
router isis Finance
 net 49.0001.aaaa.aaaa.aaaa.00
interface Ethernet 0
 ip router isis Finance
interface serial 0
 ip router isis Finance
```

The following example shows usage of the **maximum-paths** option:

```
router isis
maximum-paths?
20
```

#### Related Commands

Command	Description
<b>clns router isis</b>	Enables IS-IS routing for ISO CLNS on an interface and attaches an area designator to the routing process.
<b>ip router isis</b>	Configures an IS-IS routing process for IP on an interface and attaches an area designator to the routing process.
<b>net</b>	Configures an IS-IS NET for the routing process.
<b>redistribute (IP)</b>	Redistribute routes from one routing domain into another routing domain.
<b>route-map (IP)</b>	Defines the conditions for redistributing routes from one routing protocol into another.



# router ospf

To configure an Open Shortest Path First (OSPF) routing process, use the **router ospf** command in global configuration mode. To terminate an OSPF routing process, use the **no** form of this command.

**router ospf** *process-id* [**vrf** *vpn-name*]

**no router ospf** *process-id* [**vrf** *vpn-name*]

Syntax Description	<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>vrf</b> <i>vpn-name</i>	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with OSPF VRF processes.

**Defaults** No OSPF routing process is defined.

**Command Modes** Global configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	The <b>vrf</b> keyword and <i>vpn-name</i> arguments were added to identify a VPN.
	12.0(9)ST	The <b>vrf</b> keyword and <i>vpn-name</i> arguments were added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines** You can specify multiple OSPF routing processes in each router.

After you enter the **router ospf** command, you can enter the maximum number of paths. There can be from 1 to 32 paths.

**Examples** The following example configures an OSPF routing process and assign a process number of 109:

```
router ospf 109
```

This example shows a basic OSPF configuration using the **router ospf** command to configure OSPF VPN routing and forwarding (VRF) instance processes for the VRFs first, second, and third:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 12 vrf first
Router(config)# router ospf 13 vrf second
Router(config)# router ospf 14 vrf third
Router(config)# exit
```

The following example shows usage of the **maximum-paths** option:

```
Router> enable
Router# configure terminal
Router(config)# router ospf
Router(config-router)# maximum-paths?
Router(config)# 20
Router(config)# exit
```

---

**Related Commands**

Command	Description
<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** command in privileged EXEC mode.

**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.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## 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, gives 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.
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 percent 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 and processed locally on the router. Useful for knowing when a dead interface failed. This counter is updated only when packets are process-switched, not when packets are fast-switched.
Last output	Number of hours, minutes, and seconds since the last packet was successfully transmitted by an interface. This counter is updated only when packets are process-switched, not when packets are fast-switched.
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.

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

Field	Description
Last clearing	<p>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.</p> <p>*** indicates the elapsed time is too large to be displayed.</p> <p>0:00:00 indicates the counters were cleared more than <math>2^{31}</math> ms (and less than <math>2^{32}</math> ms) ago.</p>
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 because of a full queue.
Five minute input rate, Five minute output rate	<p>Average number of bits and packets transmitted per second in the last 5 minutes.</p> <p>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.</p>
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 minimum packet size of the medium.
giants	Number of packets that are discarded because they exceed the maximum packet size of the medium.
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.

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

Field	Description
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.
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 because of an Ethernet collision. Some collisions are normal. However, if your collision rate climbs to around 4 or 5 percent, 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 that the controller was restarted because of errors.

**Related Commands**

Command	Description
<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 Open Shortest Path First (OSPF) routing processes, use the **show ip ospf** command in EXEC mode.

**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.
	12.2(4)T	This command was modified to show packet pacing timers in the displayed output.
	12.2(15)T	This command was modified to show additional information if the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured.
	12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S and the output was expanded to display link-state advertisement (LSA) throttling timers.
	12.3(2)T	The output of this command was expanded to display LSA throttling timers and the limit on redistributed routes.
	12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and support for the Bidirectional Forwarding Detection (BFD) feature was added.
	12.0(31)S	Support for the BFD feature was added.
	12.4(4)T	Support for the BFD feature was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**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 10.0.0.1 and Domain ID 10.20.0.1
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
LSA group pacing timer 100 secs
Interface flood pacing timer 55 msecs
Retransmission pacing timer 100 msecs
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 2. 2 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has message digest authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 4. Checksum Sum 0x29BEB
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 3
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
  Area 172.16.26.0
    Number of interfaces in this area is 0
    Area has no authentication
    SPF algorithm executed 1 times
    Area ranges are
      192.168.0.0/16 Passive Advertise
    Number of LSA 1. Checksum Sum 0x44FD
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 1
    Number of indication LSA 1
    Number of DoNotAge LSA 0
    Flood list length 0

```

### Cisco IOS Release 12.2(18)SXE, 12.0(31)S, and 12.4(4)T

The following is sample output from the **show ip ospf** command to verify that the BFD feature has been enabled for OSPF process 123. The relevant command output is shown in bold in the output.

Router# **show ip ospf**

```

Routing Process "ospf 123" with ID 172.16.10.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
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
BFD is enabled
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 00:00:03.708 ago
    SPF algorithm executed 27 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x00AEF1
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0

```



Flood list length 0

Table 3 describes the significant fields shown in the display.

**Table 3** *show ip ospf Field Descriptions*

Field	Description
Routing process “ospf 201” with ID 10.0.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
SPF schedule delay	Delay time of SPF calculations.
Minimum LSA interval	Minimum interval between link-state advertisements.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router.
External flood list length	External flood list length.
BFD is enabled	BFD has been enabled on the OSPF process.

The following is an excerpt of output from the **show ip ospf** command when the OSPF Forwarding Address Suppression in Type-5 LSAs feature is configured:

```
Router# show ip ospf
.
.
Area 2
  Number of interfaces in this area is 4
  It is a NSSA area
  Perform type-7/type-5 LSA translation, suppress forwarding address
.
.
Routing Process "ospf 1" with ID 192.168.0.1
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msecs
  Minimum hold time between two consecutive SPFs 10000 msecs
  Maximum wait time between two consecutive SPFs 10000 msecs
  Incremental-SPF disabled
  Minimum LSA interval 5 secs
  Minimum LSA arrival 1000 msecs
  LSA group pacing timer 240 secs
  Interface flood pacing timer 33 msecs
  Retransmission pacing timer 66 msecs
  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 0. 0 normal 0 stub 0 nssa
External flood list length 0

```

Table 4 describes the significant fields shown in the display.

**Table 4** *show ip ospf Field Descriptions*

Field	Description
Area	OSPF area and tag.
Number of interfaces...	Number of interfaces configured in the area.
It is...	Possible types are internal, area border, or autonomous system boundary.
Routing process “ospf 1” with ID 192.168.0.1	Process ID and OSPF router ID.
Supports...	Number of types of service supported (Type 0 only).
Initial SPF schedule delay	Delay time of SPF calculations at startup.
Minimum hold time	Minimum hold time between consecutive SPF calculations.
Maximum wait time	Maximum wait time between consecutive SPF calculations.
Incremental-SPF	Status of incremental SPF calculations.
Minimum LSA...	Minimum time interval (in seconds) between link-state advertisements, and maximum arrival time (in milliseconds) of link-state advertisements.
LSA group pacing timer	Configured LSA group pacing timer (in seconds).
Interface flood pacing timer	Configured LSA flood pacing timer (in milliseconds).
Retransmission pacing timer	Configured LSA retransmission pacing timer (in milliseconds).
Number of...	Number and type of link-state advertisements that have been received.
Number of external LSA	Number of external link-state advertisements.
Number of opaque AS LSA	Number of opaque link-state advertisements.
Number of DCbitless external and opaque AS LSA	Number of demand circuit external and opaque link-state advertisements.
Number of DoNotAge external and opaque AS LSA	Number of do not age external and opaque link-state advertisements.
Number of areas in this router is	Number of areas configured for the router listed by type.
External flood list length	External flood list length.

The following is sample output from the **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. Shortest Path First (SPF) throttling was configured with the **timers throttle spf** command.

```

Router# show ip ospf 1

Routing Process "ospf 1" with ID 10.0.0.1
Supports only single TOS(TOS0) routes
Supports opaque LSA

```

```

Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs

```

Table 5 describes the significant fields shown in the display.

**Table 5** *show ip ospf Field Descriptions*

Field	Description
Routing process "ospf 1" with ID 10.0.0.1	Process ID and OSPF router ID.
Supports ...	Number of Types of Service (TOS) supported.
It is ...	Possible types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.
Maximum limit of redistributed prefixes	Value set in the <b>redistribution maximum-prefix</b> command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the <b>redistribution maximum-prefix</b> command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before initial SPF schedule for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Minimum hold time between two consecutive SPF's	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Maximum wait time between two consecutive SPF's	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```

Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPF's 10000 msecs
Maximum wait time between two consecutive SPF's 10000 msecs
Incremental-SPF disabled
Initial LSA throttle delay 100 msecs
Minimum hold time for LSA throttle 10000 msecs

```

```

Maximum wait time for LSA throttle 45000 msecs
Minimum LSA arrival 1000 msecs
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msecs
Retransmission pacing timer 66 msecs
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 24
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 04:28:18.396 ago
    SPF algorithm executed 8 times
    Area ranges are
    Number of LSA 4. Checksum Sum 0x23EB9
    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

```

The following is sample output from the **show ip ospf** command. In this example, the user had configured the **redistribution maximum-prefix** command to set a limit of 2000 redistributed routes. SPF throttling was configured with the **timers throttle spf** command.

```

Router# show ip ospf 1

Routing Process "ospf 1" with ID 192.42.110.200
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
It is an autonomous system boundary router
Redistributing External Routes from,
    static, includes subnets in redistribution
    Maximum limit of redistributed prefixes 2000
    Threshold for warning message 75%
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs

```

Table 6 describes the significant fields shown in the display.

**Table 6** *show ip ospf Field Descriptions*

Field	Description
Routing process “ospf 1” with ID 192.42.110.200	Process ID and OSPF router ID.
Supports ...	Number of TOS supported.
It is ...	Possible types are internal, area border, or autonomous system boundary.
Redistributing External Routes from	Lists of redistributed routes, by protocol.

**Table 6** *show ip ospf Field Descriptions (continued)*

Field	Description
Maximum limit of redistributed prefixes	Value set in the <b>redistribution maximum-prefix</b> command to set a limit on the number of redistributed routes.
Threshold for warning message	Percentage set in the <b>redistribution maximum-prefix</b> command for the threshold number of redistributed routes needed to cause a warning message. The default is 75 percent of the maximum limit.
Initial SPF schedule delay	Delay (in milliseconds) before the initial SPF schedule for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Minimum hold time between two consecutive SPFs	Minimum hold time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Maximum wait time between two consecutive SPFs	Maximum wait time (in milliseconds) between two consecutive SPF calculations for SPF throttling. Configured with the <b>timers throttle spf</b> command.
Number of areas	Number of areas in router, area addresses, and so on.

The following is sample output from the **show ip ospf** command. In this example, the user had configured LSA throttling, and those lines of output are displayed in bold.

```
Router# show ip ospf 1

Routing Process "ospf 4" with ID 10.10.24.4
  Supports only single TOS(TOS0) routes
  Supports opaque LSA
  Supports Link-local Signaling (LLS)
  Initial SPF schedule delay 5000 msec
  Minimum hold time between two consecutive SPFs 10000 msec
  Maximum wait time between two consecutive SPFs 10000 msec
  Incremental-SPF disabled
  Initial LSA throttle delay 100 msec
  Minimum hold time for LSA throttle 10000 msec
  Maximum wait time for LSA throttle 45000 msec
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
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 24
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm last executed 04:28:18.396 ago
    SPF algorithm executed 8 times
    Area ranges are
    Number of LSA 4. Checksum Sum 0x23EB9
    Number of opaque link LSA 0. Checksum Sum 0x0
    Number of DCbitless LSA 0
```

```
show ip ospf
```

```
Number of indication LSA 0  
Number of DoNotAge LSA 0  
Flood list length 0
```

# show ip route

To display the current state of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

**show ip route** [*ip-address* [*mask*] [**longer-prefixes**] | *protocol* [*process-id*] | **list** [*access-list-number* | *access-list-name*] | **static download**]

Syntax Description		
<i>ip-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)	Specifies that only routes matching the <i>ip-address</i> and <i>mask</i> pair should be displayed.
<i>protocol</i>	(Optional)	The 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>hello</b> , <b>eigrp</b> , <b>isis</b> , <b>ospf</b> , and <b>rip</b> .
<i>process-id</i>	(Optional)	The number used to identify a process of the specified protocol.
<b>list</b>	(Optional)	The list keyword is required to filter output by an access list name or number.
<i>access-list-number</i>	(Optional)	Filters the displayed output from the routing table based on the specified access list name.
<i>access-list-name</i>	(Optional)	Filters the displayed output from the routing table based on the specified access list number.
<b>static</b>	(Optional)	All static routes.
<b>download</b>	(Optional)	The route installed using the AAA route download function.

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	9.2	This command was introduced.
	10.0	The “D—EIGRP, EX—EIGRP, N1—OSPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were added to the command output.
	10.3	The <i>process-id</i> argument was added.
	11.0	The <b>longer-prefixes</b> keyword was added.
	11.1	The “U—per-user static route” code was added to the command output.
	11.2	The “o—on-demand routing” code was added to the command output.
	11.3	The output from the <b>show ip route</b> <i>ip-address</i> command was enhanced to display the origination of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.

Release	Modification
12.0(1)T	The “M—mobile” code was added to the command output.
12.0(3)T	The “P—periodic downloaded static route” code was added to the command output.
12.0(4)T	The “ia—IS-IS” code was added to the command output.
12.2(2)T	The output from the <b>show ip route ip-address</b> command was enhanced to display information on the multipaths to the specified network.
12.2(13)T	The <i>egp</i> and <i>igrp</i> arguments were removed because the exterior gateway protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) are no longer available in Cisco IOS software.
12.3(2)T	The output from the <b>show ip route</b> command was enhanced to display route tag information.
12.3(8)T	The output from the <b>show ip route</b> command was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

### Usage Guidelines

The **show ip route static download** command provides a way to display all dynamic static routes with name and distance information, including active and inactive ones. You can display all active dynamic static routes with both the **show ip route** and **show ip route static** commands after these active routes are added in the main routing table.

### Examples

#### Routing Table Examples

The following examples show the standard routing tables displayed by the **show ip route** command. Use the codes displayed at the beginning of each report and the information in [Table 7](#) to understand the type of route.

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,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
```

```
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
```

```
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E   10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E   10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E   10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E   10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E   10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
```



```

E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2

```

The following is sample output that includes 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,
        * - candidate default route, IA - OSPF inter area route,
        i - IS-IS derived, ia - IS-IS, U - per-user static route,
        o - on-demand routing, M - mobile, P - periodic downloaded static route,
        D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
        E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
        N2 - OSPF NSSA external type 2 route

```

Gateway of last resort is not set

```

          10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C          10.89.64.0 255.255.255.0 is possibly down,
            routing via 0.0.0.0, Ethernet0
i L2       10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2       10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0

```

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 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes
```

```

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,
        i - IS-IS derived, ia - IS-IS, U - per-user static route,
        o - on-demand routing, M - mobile, P - periodic downloaded static route,
        D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
        E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
        N2 - OSPF NSSA external type 2 route

```

Gateway of last resort is not set

```

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0

```

## ■ show ip route

```

S    10.128.0.0 is directly connected, Ethernet0
    10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C    10.19.64.0 is directly connected, Ethernet0
    10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C    10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S    10.69.0.0 255.255.0.0 is directly connected, Ethernet0

```

The following examples display all downloaded static routes. A P designates which route was installed using AAA route download.

Router# **show ip route**

```

Codes: C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

```

Gateway of last resort is 172.21.17.1 to network 0.0.0.0

```

    172.31.0.0/32 is subnetted, 1 subnets
P    172.31.229.41 is directly connected, Dialer1 20.0.0.0/24 is subnetted, 3 subnets
P    10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P    10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P    10.1.2.0 [200/0] via 172.31.229.41, Dialer1

```

Router# **show ip route static**

```

    172.27.4.0/8 is variably subnetted, 2 subnets, 2 masks
P    172.1.1.1/32 is directly connected, BRI0
P    172.27.4.0/8 [1/0] via 103.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.21.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
    172.21.0.0/16 is variably subnetted, 5 subnets, 2 masks
S    172.21.114.201/32 is directly connected, BRI0
S    172.21.114.205/32 is directly connected, BRI0
S    172.21.114.174/32 is directly connected, BRI0
S    172.21.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/8 is directly connected, BRI0
P    10.2.2.0/8 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.21.114.65, Ethernet0
S    172.29.0.0/16 [1/0] via 172.21.114.65, Ethernet0

```

The following example shows how to use the **show ip route static download** command to display all active and inactive routes installed using AAA route download:

Router# **show ip route static download**

Connectivity: A - Active, I - Inactive

```

A    10.10.0.0 255.0.0.0 BRI0
A    10.11.0.0 255.0.0.0 BRI0
A    10.12.0.0 255.0.0.0 BRI0
A    10.13.0.0 255.0.0.0 BRI0
I    10.20.0.0 255.0.0.0 172.21.1.1
I    10.22.0.0 255.0.0.0 Serial0
I    10.30.0.0 255.0.0.0 Serial0
I    10.31.0.0 255.0.0.0 Serial1
I    10.32.0.0 255.0.0.0 Serial1
A    10.34.0.0 255.0.0.0 192.168.1.1

```

```

A      10.36.1.1 255.255.255.255 BRI0 200 name remotel
I      10.38.1.9 255.255.255.0 192.168.69.1

```

**Table 7** *show ip route Field Descriptions*

Field	Description
O	<p>Indicates the protocol that derived the route. It can be one of the following values:</p> <p>I—Interior Gateway Routing Protocol (IGRP) derived</p> <p>R—Routing Information Protocol (RIP) derived</p> <p>O—Open Shortest Path First (OSPF) derived</p> <p>C—connected</p> <p>S—static</p> <p>E—Exterior Gateway Protocol (EGP) derived</p> <p>B—Border Gateway Protocol (BGP) derived</p> <p>D—Enhanced Interior Gateway Routing Protocol (EIGRP)</p> <p>EX—EIGRP external</p> <p>i—IS-IS derived</p> <p>ia—IS-IS</p> <p>M—mobile</p> <p>P—periodic downloaded static route</p> <p>U—per-user static route</p> <p>o—on-demand routing</p>
E2	<p>Type of route. It can be one of the following values:</p> <p>*—Indicates the last path used when a packet was forwarded. It pertains only to the nonfast-switched packets. However, it does not indicate which path will be used next when forwarding a nonfast-switched packet, except when the paths are equal cost.</p> <p>IA—OSPF interarea route</p> <p>E1—OSPF external type 1 route</p> <p>E2—OSPF external type 2 route</p> <p>L1—IS-IS Level 1 route</p> <p>L2—IS-IS Level 2 route</p> <p>N1—OSPF not-so-stubby area (NSSA) external type 1 route</p> <p>N2—OSPF NSSA external type 2 route</p>
10.110.0.0	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 10.119.254.6	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.

### Specific Route Information

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 10.0.0.1:

```
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 10.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
      Route metric is 20, traffic share count is 1
    10.191.255.251, from 10.191.255.247, via Fddi1/0
      Route metric is 20, traffic share count is 1
```

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 example above 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 10.191.255.247.

[Table 8](#) describes the significant fields shown when using the **show ip route** command with an IP address (previous displays).

**Table 8** *show ip route with Address Field Descriptions*

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Tag	Integer that is used to implement the route.
type	Indicates the IS-IS route type (Level 1 or Level 2).
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	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.
Routing Descriptor Blocks:	Displays the next hop IP address followed by the information source.
Route metric	This value is the best metric for this routing descriptor block.
traffic share count	Number of uses for this routing descriptor block.

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 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared to that result of 10.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Router# show ip route 10.0.0.0 10.0.0.0 longer-prefixes
```

```
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,
        i - IS-IS derived, ia - IS-IS, U - per-user static route,
        o - on-demand routing, M - mobile, P - periodic downloaded static route,
        D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
        E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
        N2 - OSPF NSSA external type 2 route
```

Gateway of last resort is not set

```
S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
    10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C    10.19.64.0 is directly connected, Ethernet0
    10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C    10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S    10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following output includes the tag 120 applied to the route 10.22.0.0/16. You must specify an IP prefix in order to see the tag value.

```
Router# show ip route 10.22.0.0
```

```
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
      Route metric is 12, traffic share count is 1
      Route tag 120
```

### Static Routes Using a DHCP Gateway Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.2.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate.

Router# **show ip route**

```
Codes: C - connected, S - static, 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
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

Gateway of last resort is 10.0.19.14 to network 0.0.0.0

```
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.2.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0

S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

#### Related Commands

Command	Description
<b>show dialer</b>	Displays general diagnostic information for interfaces configured for DDR.
<b>show interfaces tunnel</b>	Displays a list of 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 Resource Reservation Protocol (RSVP) terminal point information for receivers or senders, use the **show ip rsvp host** command in user EXEC or privileged EXEC mode.

**show ip rsvp host** { **senders** | **receivers** } [*hostname* | *ip-address*]

## Syntax Description

<b>senders</b>	Displays information for senders.
<b>receivers</b>	Displays information for receivers.
<i>hostname</i>	(Optional) Restricts the display to sessions with <i>hostname</i> as their destination.
<i>ip-address</i>	(Optional) Restricts the display to sessions with the specified IP address as their destination.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Examples

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

Router# **show ip rsvp host receivers**

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

[Table 9](#) describes the significant fields shown in the display.

**Table 9** *show ip rsvp host Field Descriptions*

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

■ show ip rsvp host

**Table 9**      *show ip rsvp host Field Descriptions (continued)*

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

**Related Commands**

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



# show ip rsvp interface

To display Resource Reservation Protocol (RSVP)-related information, use the **show ip rsvp interface** command in privileged EXEC mode.

**show ip rsvp interface** [*interface-type interface-number*] [**detail**]

Syntax Description	<i>interface-type</i>	(Optional) Type of the interface.
	<i>interface-number</i>	(Optional) Number of the interface.
	<b>detail</b>	(Optional) Additional information about interfaces.

Command Modes	Privileged EXEC
---------------	-----------------

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(2)T	The optional <b>detail</b> keyword was added.
	12.2(4)T	This command was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(13)T	The following modifications were made to this command: <ul style="list-style-type: none"> <li>Rate-limiting and refresh-reduction information were added to the output display.</li> <li>This command was modified to display RSVP global settings when no keywords or arguments are entered.</li> </ul>
	12.2(15)T	The following modifications were made to this command: <ul style="list-style-type: none"> <li>The command output was modified to display the effects of compression on admission control and the RSVP bandwidth limit counter.</li> <li>Cryptographic authentication parameters were added to the display.</li> </ul>
	12.2(18)SFX2	This command was integrated into Cisco IOS Release 12.2(18)SFX2.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines	Use the <b>show ip rsvp interface</b> command to display information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. Enter the optional <b>detail</b> keyword for additional information, including bandwidth and signaling parameters and blockade state.
------------------	--

Use the **show ip rsvp interface detail** command to display information about the RSVP parameters associated with an interface. These parameters include the following:

- Total RSVP bandwidth
- RSVP bandwidth allocated to existing flows
- Maximum RSVP bandwidth that can be allocated to a single flow

- The type of admission control supported (header compression methods)
- The compression methods supported by RSVP compression prediction

## Examples

The following command shows information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface
```

```
interface    allocated  i/f max  flow max  sub max
PO0/0        0          200M     200M      0
PO1/0        0          50M      50M       0
PO1/1        0          50M      50M       0
PO1/2        0          50M      50M       0
PO1/3        0          50M      50M       0
Lo0          0          200M     200M      0
```

Table 10 describes the fields shown in the display.

**Table 10** *show ip rsvp interface Field Descriptions*

Field	Description
interface	Interface name.
allocated	Current allocation budget.
i/f max	Maximum allocatable bandwidth.
flow max	Largest single flow allocatable on this interface.
sub max	Largest sub-pool value allowed on this interface.

## Detailed RSVP Information Example

The following command shows detailed RSVP information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface detail
```

```
PO0/0:
```

```
Bandwidth:
```

```
  Curr allocated:0 bits/sec
  Max. allowed (total):200M bits/sec
  Max. allowed (per flow):200M bits/sec
  Max. allowed for LSP tunnels using sub-pools:0 bits/sec
  Set aside by policy (total):0 bits/sec
```

```
Signalling:
```

```
  DSCP value used in RSVP msgs:0x3F
  Number of refresh intervals to enforce blockade state:4
  Number of missed refresh messages:4
  Refresh interval:30
```

```
PO1/0:
```

```
Bandwidth:
```

```
  Curr allocated:0 bits/sec
  Max. allowed (total):50M bits/sec
  Max. allowed (per flow):50M bits/sec
  Max. allowed for LSP tunnels using sub-pools:0 bits/sec
  Set aside by policy (total):0 bits/sec
```

```
Signalling:
```

```
  DSCP value used in RSVP msgs:0x3F
  Number of refresh intervals to enforce blockade state:4
  Number of missed refresh messages:4
```

```
Refresh interval:30

PO1/1:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

PO1/2:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/secMax. allowed for LSP tunnels using sub-pools:0
bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

PO1/3:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

Lo0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):200M bits/sec
    Max. allowed (per flow):200M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30
```

Table 11 describes the significant fields shown in the detailed display for interface PO0/0. The fields for the other interfaces are similar.

**Table 11** *show ip rsvp interface detail Field Descriptions –Detailed RSVP Information Example*

Field	Description
PO0/0	Interface name.
Bandwidth	<p>The RSVP bandwidth parameters in effect including the following:</p> <ul style="list-style-type: none"> <li>• Curr allocated = amount of bandwidth currently allocated in bits per second.</li> <li>• Max. allowed (total) = maximum amount of bandwidth allowed in bits per second.</li> <li>• Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second.</li> <li>• Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for label switched path (LSP) tunnels in bits per second.</li> <li>• Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.</li> </ul>
Signalling	<p>The RSVP signalling parameters in effect including the following:</p> <ul style="list-style-type: none"> <li>• DSCP value used in RSVP msgs = differentiated services code point (DSCP) used in RSVP messages.</li> <li>• Number of refresh intervals to enforce blockade state = how long in milliseconds before the blockade takes effect.</li> <li>• Number of missed refresh messages = how many refresh messages until the router state expires.</li> <li>• Refresh interval = how long in milliseconds until a refresh message is sent.</li> </ul>

### RSVP Compression Method Prediction Example

The following example from the **show ip rsvp interface detail** command shows the RSVP compression method prediction configuration for each interface on which RSVP is configured:

```
Router# show ip rsvp interface detail
```

```
Et2/1:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:0. Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled
```

```

Se3/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:1. Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled

```

Table 12 describes the significant fields shown in the display for interface Ethernet2/1. The fields for interface Serial3/0 are similar.

**Table 12** *show ip rsvp interface detail Field Descriptions—RSVP Compression Method Prediction Example*

Field	Description
Et2/1: Se3/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: <ul style="list-style-type: none"> <li>• Curr allocated = amount of bandwidth currently allocated in bits per second.</li> <li>• Max. allowed (total) = maximum amount of bandwidth allowed in bits per second.</li> <li>• Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second.</li> <li>• Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second.</li> <li>• Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.</li> </ul>
Admission Control	The type of admission control in effect including the following: <ul style="list-style-type: none"> <li>• Header Compression methods supported: <ul style="list-style-type: none"> <li>– Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes and the number of bytes saved per packet.</li> </ul> </li> </ul>
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).
Authentication	Authentication is either enabled (active) or disabled (inactive).

### Cryptographic Authentication Example

The following example of the **show ip rsvp interface detail** command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on the router:

```
Router# show ip rsvp interface detail
```

```
Et0/0:
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Neighbors:
    Using IP encap: 0. Using UDP encap: 0
  Signalling:
    Refresh reduction: disabled
  Authentication: enabled
    Key: 11223344
    Type: sha-1
    Window size: 2
    Challenge: enabled
```

Table 13 describes the significant fields shown in the display.

**Table 13** *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example*

Field	Description
Et0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: <ul style="list-style-type: none"> <li>• Curr allocated = amount of bandwidth currently allocated in bits per second.</li> <li>• Max. allowed (total) = maximum amount of bandwidth allowed in bits per second.</li> <li>• Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second.</li> <li>• Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second.</li> <li>• Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.</li> </ul>
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).

**Table 13** *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example (continued)*

Field	Description
Authentication	<p>Authentication is either enabled (active) or disabled (inactive). The parameters include the following:</p> <ul style="list-style-type: none"> <li>• <b>Key</b> = The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or encrypted &lt;encrypted&gt;.</li> <li>• <b>Type</b> = The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.</li> <li>• <b>Window size</b> = Maximum number of RSVP authenticated messages that can be received out of order.</li> <li>• <b>Challenge</b> = The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are <b>enabled</b> (active) or <b>disabled</b> (inactive).</li> </ul>

#### Related Commands

Command	Description
<b>show ip rsvp installed</b>	Displays RSVP-related installed filters and corresponding bandwidth information.
<b>show ip rsvp neighbor</b>	Displays current RSVP neighbors.

# show mpls traffic-eng autoroute

To display tunnels announced to the Interior Gateway Protocol (IGP), including interface, destination, and bandwidth, use the **show mpls traffic-eng autoroute** command in user EXEC or privileged EXEC mode.

## show mpls traffic-eng autoroute

### Defaults

No default behavior or values

### Command Modes

User EXEC  
Privileged EXEC

### Command History

Release	Modification
12.0(5)S	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

### Usage Guidelines

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

### Examples

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

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

```
Router# show mpls traffic-eng autoroute
```

```
MPLS TE autorouting enabled
destination 0002.0002.0002.00 has 2 tunnels
  Tunnel1021 (traffic share 10000, nexthop 10.2.2.2, absolute metric 11)
  Tunnel1022 (traffic share 3333, nexthop 10.2.2.2, relative metric -3)
destination 0003.0003.0003.00 has 2 tunnels
  Tunnel1032 (traffic share 10000, nexthop 172.16.3.3)
  Tunnel1031 (traffic share 10000, nexthop 172.16.3.3, relative metric -1)
```

[Table 14](#) describes the significant fields shown in the display.

**Table 14** *show mpls traffic-eng autoroute Field Descriptions*

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



**Table 14** *show mpls traffic-eng autoroute Field Descriptions (continued)*

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

**Related Commands**

Command	Description
<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 (FRR) database, use the **show mpls traffic-eng fast-reroute database** command in EXEC mode.

```
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 | complete}] [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>mask length</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>	(Optional) Shows only database entries related to the backup outgoing interface.
	<i>ifname</i>	Name of the backup outgoing interface.
	<b>state</b>	(Optional) Shows entries that match one of four possible states: partial, complete, ready, or active.
	<b>active</b>	(Optional) The FRR rewrite has been put into the forwarding database (where it can be placed onto appropriate incoming packets).
	<b>ready</b>	(Optional) The FRR rewrite has been created, but has not yet been moved into the forwarding database.
	<b>partial</b>	(Optional) 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>role</b>	(Optional) Shows entries associated either with the tunnel head or tunnel midpoint.
	<b>head</b>	(Optional) Entry associated with tunnel head.
	<b>middle</b>	(Optional) Entry associated with tunnel midpoint.
	<b>detail</b>	(Optional) Shows long-form information: LFIB-FRR total number of clusters, groups and items in addition to the short-form information of prefix, label and state.

**Defaults** No default behavior or values.

**Command Modes** EXEC

Command History	Release	Modification
	12.0(10)ST	This command was introduced.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SX.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**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 10.0.0.0
```

Tunnel head fast reroute information:

Prefix	Tunnel	In-label	Out intf/label	FRR intf/label	Status
10.0.0.0/16	Tu111	Tun hd	PO0/0:Untagged	Tu4000:16	ready
10.0.0.0/16	Tu449	Tun hd	PO0/0:Untagged	Tu4000:736	ready
10.0.0.0/16	Tu314	Tun hd	PO0/0:Untagged	Tu4000:757	ready
10.0.0.0/16	Tu313	Tun hd	PO0/0:Untagged	Tu4000:756	ready

Table 15 describes significant fields shown in the display.

**Table 15** *show mpls traffic-eng fast-reroute database Field Descriptions*

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	<p>Out interface—short name of the physical interface through which traffic goes to the protected link.</p> <p>Out label:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> </ul>

**Table 15** *show mpls traffic-eng fast-reroute database Field Descriptions (continued)*

Field	Description
FRR intf/label	Fast Reroute interface—the backup tunnel interface.  Fast Reroute label <ul style="list-style-type: none"> <li>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.</li> <li>At tunnel midpoints, this has the same value as the Out Label.</li> </ul>
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** keyword 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    Outintf/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          PO0/0:694        Tu4000:694        active
10.110.0.10 228 [7332] 254          PO0/0:693        Tu4000:693        active
10.110.0.10 227 [7331] 253          PO0/0:692        Tu4000:692        active
10.110.0.10 226 [7334] 252          PO0/0:691        Tu4000:691        active
10.110.0.10 225 [7333] 251          PO0/0:690        Tu4000:690        active
10.110.0.10 224 [7329] 250          PO0/0:689        Tu4000:689        active
```

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

```
Router# show mpls traffic-eng fast-reroute database 10.0.0.0. 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 PO0/0:773, FRR label Tu4000:773
Prefix 12.0.0.0/16, Tu392, active
Input label Tun hd, Output label PO0/0:775, FRR label Tu4000:775
Prefix 12.0.0.0/16, Tu111, active
Input label Tun hd, Output label PO0/0:16, FRR label Tu4000:16
Prefix 12.0.0.0/16, Tu394, active
Input label Tun hd, Output label PO0/0:774, FRR label Tu4000:774
```

Table 16 describes significant fields when the **detail** keyword is used.

**Table 16** *show mpls traffic-eng fast-reroute database with detail Keyword Field Descriptions*

Field	Description
Total Clusters	A cluster is the physical interface upon which Fast Reroute link protection has been enabled.
Total Groups	<p>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.</p> <p>For example, the cluster Ethernet4/0/1 is protected by backup Tunnel1 and backup Tunnel2, and so has two groups.</p>
Total Items	An item is a database record that associates a rewrite with a group. A group therefore can have one or more items.
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
<b>show mpls traffic-eng fast-reroute log reroutes</b>	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** command in EXEC mode.

## 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.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SX.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**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 msec	Suspends	Errors
00:27:39	PO0/0	Down	1079	30 msec	30	0	0
00:27:35	PO0/0	Up	1079	40 msec	40	0	0

[Table 17](#) describes significant fields shown in the display.

**Table 17** *show mpls traffic-eng fast-reroute log reroutes Field Descriptions*

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 msec	CPU time spent processing those reroutes. (This is less than or equal to the Duration value).

**Table 17** *show mpls traffic-eng fast-reroute log reroutes Field Descriptions (continued)*

Display Field	Description
Suspends	Number of times that reroute processing for this event was interrupted to let the CPU handle other tasks.
Errors	Number of unsuccessful reroute attempts.

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

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

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

<b>Syntax Description</b>	<i>interface-name</i> (Optional) Displays only tunnels that were admitted on the specified interface.
---------------------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.1(3)T	The command output changed. The BW field now shows bandwidth in kbps, and it is followed by the status (reserved or held) of the bandwidth.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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

```
System Information::
```

```
  Tunnels Count:      4
```

```
  Tunnels Selected:   4
```

TUNNEL ID	UP IF	DOWN IF	PRIORITY	STATE	BW (kbps)
10.106.0.6 1000_1	AT1/0.2	-	0/0	Resv Admitted	0
10.106.0.6 2000_1	Et4/0/1	-	1/1	Resv Admitted	0
10.106.0.6 1_2	Et4/0/1	Et4/0/2	1/1	Resv Admitted	3000 R
10.106.0.6 2_2	AT1/0.2	AT0/0.2	1/1	Resv Admitted	3000 R

[Table 18](#) describes the significant fields shown in the display.

**Table 18** *show mpls traffic-eng link-management admission-control Field Descriptions*

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



**Table 18** *show mpls traffic-eng link-management admission-control Field Descriptions*

Field	Description
STATE	Admission status of the tunnel.
BW (kbps)	Bandwidth of the tunnel (in kbps). If an “R” follows the bandwidth number, the bandwidth is reserved. If an “H” follows the bandwidth number, the bandwidth is temporarily being held for a path message.

**Related Commands**

Command	Description
<b>show mpls traffic-eng link-management advertisements</b>	Displays local link information that MPLS traffic engineering link management is currently flooding 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 a summary of link management information.

# show mpls traffic-eng link-management advertisements

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

## show mpls traffic-eng link-management advertisements

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

**Command Modes** User EXEC  
Privileged EXEC

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(3)T	The command output was modified.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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

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

Table 19 describes the significant fields shown in the display.

**Table 19** *show mpls traffic-eng link-management advertisements Field Descriptions*

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

**Related Commands**

Command	Description
<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 a summary of link management information.

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

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

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

## Syntax Description

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

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	The command output was modified.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

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

## Examples

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

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

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

```

6          0          0          0          3000
7          0          0          0          3000

```

Table 20 describes the significant fields shown in the display.

**Table 20** *show mpls traffic-eng link-management bandwidth-allocation Field Descriptions*

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

#### Related Commands

Command	Description
<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 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 a summary of link management information.

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

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

**show mpls traffic-eng link-management igp-neighbors** [*igp-id* [*isis isis-address* | *ospf ospf-id*] | *ip ip-address*]

Syntax Description	<i>igp-id</i>	(Optional) Displays the IGP neighbors that are using a specified IGP identification.
	<b>isis</b> <i>isis-address</i>	(Optional) Displays the specified IS-IS neighbor when you display neighbors by IGP ID.
	<b>ospf</b> <i>ospf-id</i>	(Optional) Displays the specified OSPF neighbor when you display neighbors by IGP ID.
	<b>ip</b> <i>ip-address</i>	(Optional) Displays the IGP neighbors that are using a specified IGP IP address.

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**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: 10.0.0.0)
Link ID:: PO1/0/0
  Neighbor ID: 0000.0026.0001.00 (area: isis level-1, IP: 172.16.1.2)
```

[Table 21](#) describes the significant fields shown in the display.

**Table 21** *show mpls traffic-eng link-management igp-neighbors Field Descriptions*

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

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

# show mpls traffic-eng link-management interfaces

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

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

<b>Syntax Description</b>	<i>interface-name</i> (Optional) Displays information only for the specified interface.
---------------------------	---

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.1(3)T	The command output was modified.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Usage Guidelines</b>	Displays resource and configuration information for all configured interfaces.
-------------------------	--

<b>Examples</b>	The following is sample output from the <b>show mpls traffic-eng link-management interfaces</b> command:
-----------------	--

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

System Information::
  Links Count:          2
Link ID:: Et4/0/1 (10.1.0.6)
Link Status:
  Physical Bandwidth:  10000 kbits/sec
  Max Reservable BW:   5000 kbits/sec (reserved:0% in, 60% out)
  MPLS TE Link State:  MPLS TE on, RSVP on, admin-up, flooded
  Inbound Admission:   reject-huge
  Outbound Admission:  allow-if-room
  Admin. Weight:       10 (IGP)
  IGP Neighbor Count:  1
  IGP Neighbor:        ID 0001.0000.0001.02, IP 10.0.0.0 (Up)
Flooding Status for each configured area [1]:
  IGP Area[1]: isis level-1: flooded
```

Table 22 describes the significant fields shown in the display.



**Table 22** *show mpls traffic-eng link management interfaces Field Descriptions*

Field	Description
Links Count	Number of links that were enabled for use with Multiprotocol Label Switching (MPLS) traffic engineering.
Link ID	Index of the link.
Physical Bandwidth	Link's bandwidth capacity (in kbps).
Max Reservable BW	Amount of reservable bandwidth on this link.
MPLS TE Link State	The status of the MPLS link.
Inbound Admission	Link admission policy for inbound tunnels.
Outbound Admission	Link admission policy for outbound tunnels.
Admin. Weight	Administrative weight associated with this link.
IGP Neighbor Count	Number of Interior Gateway Protocol (IGP) neighbors directly reachable over this link.
IGP Neighbor	IGP neighbor on this link.
Flooding Status for each configured area	Flooding status for the specified configured area.

**Related Commands**

Command	Description
<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 summary</b>	Displays a summary of link management information.

# show mpls traffic-eng link-management summary

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

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

Syntax Description	<i>interface-name</i> (Optional) Displays information only for the specified interface.
--------------------	---

Command Modes	User EXEC Privileged EXEC
---------------	------------------------------

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.1(3)T	The command output was modified.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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

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

Table 23 describes the significant fields shown in the display.

**Table 23** *show mpls traffic-eng link-management summary Field Descriptions*

Field	Description
Links Count	Number of links configured for MPLS traffic engineering.
Flooding System	Enable status of the MPLS traffic engineering flooding system.
IGP Area ID	Name of the IGP area being described.
Flooding Protocol	IGP being used to flood information for this area.
Flooding Status	Status of flooding for this area.
Periodic Flooding	Status of periodic flooding for this area.
Flooded Links	Number of links that were flooded.
IGP System ID	IGP for this node associated with this area.
MPLS TE Router ID	MPLS traffic engineering router ID for this node.
IGP Neighbors	Number of reachable IGP neighbors associated with this area.
Link ID	Interface name and IP address of the link being described.
Physical Bandwidth	Link bandwidth capacity (in kbps).
Max Reservable BW	Amount of reservable bandwidth on this link.
MPLS TE Link State	Status of the link's MPLS traffic engineering-related functions.
Inbound Admission	Link admission policy for incoming tunnels.
Outbound Admission	Link admission policy for outgoing tunnels.
Admin. Weight	Link administrative weight.
IGP Neighbor Count	List of the IGP neighbors directly reachable over this link.

#### 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.
<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.

# 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** {*ip-address* | **igp-id** {*isis nsap-address* | **ospf ip-address**}} [**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 nsap-address</b>	Specifies the node by router identification ( <i>nsap-address</i> ) if using IS-IS.
	<b>ospf ip-address</b>	Specifies the node by router identifier if using OSPF.
	<b>brief</b>	(Optional) Provides a less detailed version of the topology.

Command Modes Privileged 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 “subpool.”
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

```
Router# show mpls traffic-eng topology

My_System_id: 0000.0025.0003.00

IGP Id: 0000.0024.0004.00, MPLS TE Id:172.16.4.4 Router Node
  link[0 ]:Intf Address: 10.1.1.4
                Nbr IGP Id: 0000.0024.0004.02,
                admin_weight:10, affinity_bits:0x0
                max_link_bw:10000 max_link_reservable: 10000
  globalpoolsubpool
    total allocatedreservable reservable
    -----
  bw[0]: 0 1000500
  bw[1]:10 990490
  bw[2]: 600 390390
  bw[3]: 0 390390
  bw[4]: 0 390390
  bw[5]: 0 390390
```

Table 24 describes the significant fields shown in the display.

**Table 24** *show mpls traffic-eng topology Field Descriptions*

Field	Description
My-System_id	Unique identifier of the IGP.
IGP Id	Identification of advertising router.
MPLS TE Id	Unique MPLS traffic engineering identification.
Intf Address	The interface address of the link.
Nbr IGP Id	Neighbor IGP router identifier.
admin_weight	Cost of the link.
affinity_bits	Requirements on the attributes of the links that the traffic crosses.
max_link_bw	Physical line rate.
max_link_reservable	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.

**Related Commands**

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

# show mpls traffic-eng tunnels

To show information about tunnels, use the **show mpls traffic-eng tunnels** command in user EXEC or privileged EXEC mode.

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

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

## Syntax Description

<i>tunnel-interface</i>	Displays information for the specified tunneling interface.
<b>brief</b>	(Optional) Displays the information in brief format.
<b>protect</b>	Displays the status of the protected path.
<b>destination</b> <i>address</i>	(Optional) Restricts the display to tunnels destined to the specified IP address.
<b>source-id</b>	(Optional) Restricts the display to tunnels with a matching source IP address or tunnel number.
<i>number</i>	(Optional) Tunnel number.
<i>ip-address</i>	(Optional) Source IP address.
<i>ip-address number</i>	(Optional) Source IP address and tunnel number.
<b>role</b>	(Optional) Restricts the display to tunnels with the indicated role (all, head, middle, tail, or remote).
<b>all</b>	(Optional) Displays all tunnels.
<b>head</b>	(Optional) Displays tunnels with their heads at this router.
<b>middle</b>	(Optional) Displays tunnels with their midpoints at this router.
<b>tail</b>	(Optional) Displays tunnels with their tails at this router.
<b>remote</b>	(Optional) Displays tunnels with their heads at another router; this is a combination of the <b>middle</b> and <b>tail</b> keyword values.
<b>up</b>	(Optional) Displays tunnels if the tunnel interface is up. Tunnel midpoints and tails are typically up or not present.
<b>down</b>	(Optional) Displays tunnels that are down.
<b>name</b> <i>string</i>	(Optional) Displays tunnels with the specified name. The tunnel name is derived from the interface description, if specified; otherwise, it is the interface name. The tunnel name is included in the signalling message so it is available at all hops.
<b>suboptimal constraints none</b>	(Optional) 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>	(Optional) 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.
<b>suboptimal constraints max</b>	(Optional) 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>physical-interface</i>	(Optional) Displays tunnels that use the specified input interface.
<b>interface out</b> <i>physical-interface</i>	(Optional) Displays tunnels that use the specified output interface.
<b>interface</b> <i>physical-interface</i>	(Optional) Displays tunnels that use the specified interface as an input or output interface.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(3)T	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 nonbrief format. The nonbrief, nonsummary formats each include the history of LSP selection.
12.0(30)S	The <b>protect</b> keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## 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
```

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

```
Router# show mpls traffic-eng tunnels 500 protect brief
```

```
Router#_t500
```

```

LSP Head, Tunnel500, Admin: up, Oper: up
Src 172.16.0.5, Dest 172.16.0.8, Instance 17
```

```
show mpls traffic-eng tunnels
```

```
Fast Reroute Protection: None
Path Protection: 1 Common Link(s) , 1 Common Node(s)
  Primary lsp path:192.168.6.6 192.168.7.7
                  192.168.8.8 192.168.0.8

  Protect lsp path:172.16.7.7 192.168.8.8
                  10.0.0.8
Path Protect Parameters:
  Bandwidth: 50          kbps (Global)  Priority: 7 7  Affinity: 0x0/0xFFFF
  Metric Type: TE (default)
InLabel  : -
OutLabel : Serial5/3, 46
RSVP Signalling Info:
  Src 172.16.0.5, Dst 172.16.0.8, Tun_Id 500, Tun_Instance 18
RSVP Path Info:
  My Address: 172.16.0.5
  Explicit Route: 192.168.7.7 192.168.8.8
  Record Route: NONE
  Tspec: ave rate=50 kbits, burst=1000 bytes, peak rate=50 kbits
RSVP Resv Info:
  Record Route: NONE
  Fspec: ave rate=50 kbits, burst=1000 bytes, peak rate=50 kbits
```

Table 25 describes the significant fields shown in the display.

**Table 25** *show mpls traffic-eng tunnels Field Descriptions*

Field	Description
LSP Tunnels Process	Status of the LSP tunnels process.
RSVP Process	Status of the RSVP process.
Forwarding	Status of forwarding (enabled or disabled).
Periodic reoptimization	Schedule for periodic reoptimization.
TUNNEL NAME	Name of the interface that is configured at the tunnel head.
DESTINATION	Identifier of the tailend router.
UP IF	Upstream interface that the tunnel used.
DOWN IF	Downstream interface that the tunnel used.
STATE/PROT	For tunnel heads, admin-down or up. For nonheads, signalled.

#### Related Commands

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



# tunnel destination

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

**tunnel destination** {*host-name* | *ip-address* | *ipv6-address*}

**no tunnel destination**

Syntax Description	<i>host-name</i>	Name of the host destination.
	<i>ip-address</i>	IP address of the host destination expressed in dotted decimal notation.
	<i>ipv6-address</i>	IPv6 address of the host destination expressed in IPv6 address format.

**Defaults** No tunnel interface destination is specified.

**Command Modes** Interface configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.3(7)T	The address field was modified to accept an <i>ipv6-address</i> argument to allow IPv6 nodes to be configured as a tunnel destination.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Usage Guidelines** You cannot configure two tunnels to use the same encapsulation mode with exactly the same source and destination address. The work around is to create a loopback interface and configure the packet source off of the loopback interface. Refer to the *Cisco IOS AppleTalk, DECnet, ISO CLNS, and Novell IPX Configuration Guide* for more information on AppleTalk Cayman tunneling.

## Examples Tunnel Destination Address for Cayman Tunnel Example

The following example shows how to configure the tunnel destination address for Cayman tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# tunnel source ethernet0
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode cayman
```

## Tunnel Destination Address for GRE Tunneling Example

The following example shows how to configure the tunnel destination address for GRE (generic routing encapsulation) tunneling:

```
Router(config)# interface tunnel0
Router(config-if)# appletalk cable-range 4160-4160 4160.19
Router(config-if)# appletalk zone Engineering
Router(config-if)# tunnel source ethernet0
```

```
Router(config-if)# tunnel destination 10.108.164.19
Router(config-if)# tunnel mode gre ip
```

### Tunnel Destination Address for IPv6 Tunnel Example

The following example shows how to configure the tunnel destination address for GRE (generic routing encapsulation) tunneling of IPv6 packets:

```
Router(config)# interface Tunnel0
Router(config-if)# no ip address
Router(config-if)# ipv6 router isis
Router(config-if)# tunnel source Ethernet0/0
Router(config-if)# tunnel destination 2001:0DB8:1111:2222::1/64
Router(config-if)# tunnel mode gre ipv6
Router(config-if)# exit
!
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# exit
!
Router(config)# ipv6 unicast-routing

Router(config)# router isis
Router(config)# net 49.0000.0000.000a.00
```

#### Related Commands

Command	Description
<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 Multiprotocol Label Switching (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**

<b>Syntax Description</b>	This command has no arguments or keywords.
---------------------------	--

<b>Defaults</b>	Disabled.
-----------------	-----------

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

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

<b>Examples</b>	The following example shows how to set the mode of the tunnel to MPLS traffic engineering: <pre>Router(config-if)# tunnel mode mpls traffic-eng</pre>
-----------------	--

Related Commands	Command	Description
	<b>tunnel mpls traffic-eng affinity</b>	Configures an affinity for an MPLS traffic engineering tunnel.
	<b>tunnel mpls traffic-eng autoroute announce</b>	Instructs the IGP to use the tunnel in its enhanced SPF algorithm calculation (if the tunnel is up).
	<b>tunnel mpls traffic-eng bandwidth</b>	Configures the 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 an MPLS traffic engineering tunnel.

# tunnel mpls traffic-eng affinity

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

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

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

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

Defaults	<i>properties</i> : 0X00000000 <i>mask value</i> : 0X0000FFFF
----------	--

Command Modes	Interface configuration
---------------	-------------------------

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

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

Any properties set to 1 in the affinity should also be 1 in the mask. In other words, affinity and mask should be set as follows:

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

Examples	<p>The following example shows how to set the affinity of the tunnel to 0x0101 mask 0x303:</p> <pre>Router(config-if)# tunnel mpls traffic-eng affinity 0x0101 mask 0x303</pre>
----------	---

**Related Commands**

Command	Description
<b>mpls traffic-eng attribute-flags</b>	Sets the attributes 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 specify that the Interior Gateway Protocol (IGP) should use the tunnel (if the tunnel is up) in its enhanced shortest path first (SPF) calculation, use the **tunnel mpls traffic-eng autoroute announce** 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 IGP does not use the tunnel in its enhanced SPF calculation.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

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

**Examples** The following example shows how to specify that the IGP should use the tunnel in its enhanced SPF calculation if the tunnel is up:

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

The following example shows how to specify that if the IGP is using this tunnel in its enhanced SPF calculation, the IGP should give it an absolute metric of 10:

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

Related Commands	Command	Description
	<b>ip route</b>	Establishes static routes.
	<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 Multiprotocol Label Switching (MPLS) traffic engineering tunnel metric that the Interior Gateway Protocol (IGP) enhanced shortest path first (SPF) calculation uses, use the **tunnel mpls traffic-eng autoroute metric** command in interface configuration mode. To disable the specified MPLS traffic engineering tunnel metric, 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	<b>absolute</b>	Absolute metric mode; you can enter a positive metric value.
	<b>relative</b>	Relative metric mode; you can enter a positive, negative, or zero value.
	<i>value</i>	The metric that the IGP enhanced SPF calculation uses. The <b>relative</b> value can be from -10 to 10.
	<b>Note</b>	Even though the value for a relative metric can be from -10 to 10, configuring a tunnel metric with a negative value is considered a misconfiguration. If from the routing table the metric to the tunnel tail appears to be 4, then the cost to the tunnel tail router is actually 3 because 1 is added to the cost for getting to the loopback address. In this instance, the lowest value that you can configure for the relative metric is -3.

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

**Command Modes** Interface configuration

Command History	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

**Examples** The following example shows how to specify the use of MPLS traffic engineering tunnel metric negative 1 for the IGP enhanced SPF calculation:

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

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

# tunnel mpls traffic-eng bandwidth

To configure bandwidth required for a Multiprotocol Label Switching (MPLS) traffic engineering tunnel, use the **tunnel mpls traffic-eng bandwidth** command in interface configuration mode. To disable this bandwidth configuration, use the **no** form of this command.

**tunnel mpls traffic-eng bandwidth** [**sub-pool** | **global**] *kbps*

**no tunnel mpls traffic-eng bandwidth** [**sub-pool** | **global**] *kbps*

Syntax Description	<b>sub-pool</b>	(Optional) Indicates a subpool 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 <b>sub-pool</b> keyword. But if users of pre-DiffServ-aware Traffic Engineering (DS-TE) images enter this keyword, it is accepted.
	<i>kbps</i>	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	<b>Release</b>	<b>Modification</b>
	12.0(5)S	This command was introduced.
	12.0(11)ST	The <b>sub-pool</b> keyword was added.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines	<p>Enter the bandwidth for either a global pool or subpool tunnel, not both. Only the <b>ip RSVP bandwidth</b> command specifies the two bandwidths within one command.</p> <p>To set up only a global pool tunnel, leave out the keyword <b>sub-pool</b>. If you enter <b>global</b> as a keyword, the system will accept it, but will not write it to NVRAM. This is to avoid the problem of having your configuration not understood if you upgrade to an image that contains the DS-TE capability and then return to a non-DS-TE image.</p>
------------------	---

Examples	The following example shows how to configure 100 kbps of bandwidth for the MPLS traffic engineering tunnel:
----------	---

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



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 (TE) tunnel to use an established backup tunnel in the event of a link or node failure, use the **tunnel mpls traffic-eng fast-reroute** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng fast-reroute [bw-protect]**

**no tunnel mpls traffic-eng fast-reroute**

<b>Syntax Description</b>	<b>bw-protect</b>	(Optional) Sets the “bandwidth protection desired” bit so that backup bandwidth protection is enabled.
---------------------------	-------------------	--

<b>Defaults</b>	There is no backup bandwidth protection.
-----------------	--

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

<b>Command History</b>	Release	Modification
	12.0(10)ST	This command was introduced.
	12.0(29)S	The <b>bw-protect</b> keyword was added.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

<b>Usage Guidelines</b>	If you specify the <b>bw-protect</b> keyword, all path messages for the tunnel’s label-switched path (LSP) are sent with the bandwidth protection bit set.
-------------------------	--

After you enter the command, with or without the **bw-protect** keyword, the requested action/change propagates quickly along all hops of the LSP. Midpoint routers that are point of local repairs (PLRs) for the LSP take the appropriate action based on whether the bit was just set or cleared. If the bit was just set or cleared, a new backup tunnel selection happens for the LSP since it now has a higher or lower priority in the backup tunnel selection process.

To unconfigure only backup bandwidth protection, enter **tunnel mpls traffic-eng fast-reroute**.

To disable an MPLS TE tunnel from using an established backup tunnel in the event of a link or node failure, enter the **no** format of the command.

<b>Examples</b>	In the following example, backup bandwidth protection is enabled.
-----------------	---

```
Router(config-if)# tunnel mpls traffic-eng fast-reroute bw-protect
```

**Related Commands**

Command	Description
<b>mpls traffic-eng fast-reroute backup-prot-preemption</b>	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

# tunnel mpls traffic-eng path-option

To configure a path option for a Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng path-option** command in interface configuration mode. To disable the specified path option, use the **no** form of this command.

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

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

## Syntax Description

<b>protect</b>	(Optional) Backup label-switched path (LSP.)
<i>number</i>	When multiple path options are configured, lower numbered options are preferred.
<b>dynamic</b>	Part of the LSP is dynamically calculated.
<b>explicit</b>	Part of the LSP 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>	(Optional) The LSP cannot be reoptimized.

## Defaults

Disabled.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(30)S	The <b>protect</b> keyword was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

## Usage Guidelines

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

Dynamic path protection is not recommended.

You should not configure the **lockdown** option with protected paths.

## Examples

The following example shows how to configure the tunnel to use a named IP explicit path:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit path750
```

In the following example, tunnel 10 is protected with path3441:

```
Router(config-if)# tunnel mpls traffic-eng path-option protect 10 explicit path3441
```

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>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 Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnel, use the **tunnel mpls traffic-eng priority** command in interface configuration mode. To remove the specified setup and reservation priority, use the **no** form of this command.

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

**no tunnel mpls 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 signalled. 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.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Usage Guidelines	When a label switched path (LSP) is being signaled and an interface does not currently have enough bandwidth available for that LSP, the call admission software preempts lower-priority LSPs so that the new LSP can be admitted. (LSPs are preempted if that allows the new LSP to be admitted.)
	In the described determination, the new LSP's priority is its setup priority and the existing LSP's priority is its hold priority. The two priorities make it possible to signal an LSP with a low setup priority (so that the LSP does not preempt other LSPs on setup) but a high hold priority (so that the LSP is not preempted after it is established).
	Setup priority and hold priority are typically configured to be equal, and setup priority cannot be better (numerically smaller) than the hold priority.

Examples	The following example shows how to configure a tunnel with a setup and hold priority of 1:
	Router(config-if)# <b>tunnel mpls traffic-eng priority 1</b>

**Related Commands**

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

# Glossary

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

**AS**—Autonomous System. A collection of networks under a common administration, sharing a common routing strategy and identified by a unique 16-bit number (assigned by the Internet Assigned Numbers Authority).

**BGP**—Border Gateway Protocol. The predominant interdomain routing protocol. It is defined by RFC 1163. Version 4 uses route aggregation mechanisms to reduce the size of routing tables.

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

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 DiffServ 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.

**IS-IS**—Intermediate System-to-Intermediate System. A link-state hierarchical routing protocol, based on DECnet Phase V routing, whereby nodes exchange routing information based on a single metric, to determine network topology.

**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.



Note

See *Internetworking Terms and Acronyms* for terms not included in this glossary.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2002, 2006 Cisco Systems, Inc. All rights reserved

