

## show xtagatm cos-bandwidth-allocation xtagatm

To display information about quality of service (QoS) bandwidth allocation on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm cos-bandwidth-allocation xtagatm** command in user EXEC or privileged EXEC mode.

```
show xtagatm cos-bandwidth-allocation xtagatm [xtagatm interface number]
```

### Syntax Description

**xtagatm interface number** (Optional) Specifies the XTagATM interface number.

### Defaults

Available 50 percent, control 50 percent.

### Command Modes

User EXEC  
Privileged EXEC

### Command History

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

### Usage Guidelines

Use this command to display QoS bandwidth allocation information for the following QoS traffic categories:

- Available
- Standard
- Premium
- Control

### Examples

The following example shows output from this command:

```
Router# show xtagatm cos-bandwidth-allocation xtagatm 123
```

```
CoS           Bandwidth allocation
available     25%
standard      25%
premium       25%
control       25%
```

# show xtagatm cross-connect

To display information about the Label Switch Controller (LSC) view of the cross-connect table on the remotely controlled ATM switch, use the **show xtagatm cross-connect** command in user EXEC or privileged EXEC mode.

```
show xtagatm cross-connect [traffic] [interface interface [vpi vci] | descriptor descriptor
                             [vpi vci]]
```

Syntax Description		
<i>traffic</i>	(Optional)	Displays receive and transmit cell counts for each connection.
<b>interface</b> <i>interface</i>	(Optional)	Displays only connections with an endpoint of the specified interface.
<i>vpi vci</i>	(Optional)	Displays only detailed information on the endpoint with the specified virtual path identifier (VPI)/virtual channel identifier (VCI) on the specified interface.
<b>descriptor</b> <i>descriptor</i>	(Optional)	Displays only connections with an endpoint on the interface with the specified physical descriptor.

Command Modes	
	User EXEC Privileged EXEC

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

**Examples** Each connection is listed twice in the output from the **show xtagatm cross-connect** command, because it shows each interface that is linked by the connection.

The following is sample output from the **show xtagatm cross-connect** command:

```
Router# show xtagatm cross-connect

Phys Desc      VPI/VCI      Type      X-Phys Desc  X-VPI/VCI    State
-----
10.1.1.0       1/37         ->        10.3.0       1/35         UP
10.1.1.0       1/34         ->        10.3.0       1/33         UP
10.1.1.0       1/33         <->       10.2.0       0/32         UP
10.1.1.0       1/32         <->       10.3.0       0/32         UP
10.1.1.0       1/35         <-        10.3.0       1/34         UP
10.2.2.0       1/57         ->        10.3.0       1/49         UP
10.2.2.0       1/53         ->        10.3.0       1/47         UP
10.2.2.0       1/48         <-        10.1.1.0     1/50         UP
10.2.2.0       0/32         <->       10.1.1.0     1/33         UP
10.3.0         1/34         ->        10.1.1.0     1/35         UP
10.3.0         1/49         <-        10.2.0       1/57         UP
10.3.0         1/47         <-        10.2.0       1/53         UP
10.3.0         1/37         <-        10.1.1.0     1/38         UP
10.3.0         1/35         <-        10.1.1.0     1/37         UP
10.3.0         1/33         <-        10.1.1.0     1/34         UP
10.3.0         0/32         <->       10.1.1.0     1/32         UP
```

Table 67 describes the significant fields shown in the display.

**Table 67** show xtagatm cross-connect Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
Type	The type can be one of the following: A right arrow (->) indicates an ingress endpoint, where traffic is received into the switch. A left arrow (<-) indicates an egress endpoint, where traffic is transmitted from the interface. A bidirectional arrow (<->) indicates that traffic is both transmitted and received at this endpoint.
X-Phys Desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
State	Indicates the status of the cross-connect to which this endpoint belongs. The state is typically UP; other values, all of which are transient, include the following: <ul style="list-style-type: none"> <li>• DOWN</li> <li>• ABOUT_TO_DOWN</li> <li>• ABOUT_TO_CONNECT</li> <li>• CONNECTING</li> <li>• ABOUT_TO_RECONNECT</li> <li>• RECONNECTING</li> <li>• ABOUT_TO_RESYNC</li> <li>• RESYNCING</li> <li>• NEED_RESYNC_RETRY</li> <li>• ABOUT_TO_RESYNC_RETRY</li> <li>• RETRYING_RESYNC</li> <li>• ABOUT_TO_DISCONNECT</li> <li>• DISCONNECTING</li> </ul>

The following is sample output from the **show xtagatm cross-connect** command for a single endpoint:

```
Router# show xtagatm cross-connect descriptor 10.1.0 1 42

Phys desc: 10.1.0
Interface: n/a
Intf type: switch control port
VPI/VCI: 1/42
X-Phys desc: 10.2.0
X-Interface: XTagATM0
X-Intf type: extended tag ATM
```

```

X-VPI/VCI: 2/38
Conn-state: UP
Conn-type: input/output
Cast-type: point-to-point
Rx service type: Tag COS 0
Rx cell rate: n/a
Rx peak cell rate: 10000
Tx service type: Tag COS 0
Tx cell rate: n/a
Tx peak cell rate: 10000
    
```

Table 68 describes the significant fields shown in the display.

**Table 68** show xtagatm cross-connect descriptor Field Descriptions

Field	Description
Phys desc	Physical descriptor. A switch-supplied string identifying the interface on which the endpoint exists.
Interface	The (Cisco IOS) interface name.
Intf type	Interface type. Can be either extended Multiprotocol Label Switched (MPLS) ATM (XTagATM) or a switch control port.
VPI/VCI	Virtual path identifier and virtual channel identifier for this endpoint.
X-Phys desc	Physical descriptor for the interface of the other endpoint belonging to the cross-connect.
X-Interface	The (Cisco IOS) name for the interface of the other endpoint belonging to the cross-connect.
X-Intf type	Interface type for the interface of the other endpoint belonging to the cross-connect.
X-VPI/VCI	Virtual path identifier and virtual channel identifier of the other endpoint belonging to the cross-connect.
Conn-state	Indicates the status of the cross-connect to which this endpoint belongs. The cross-connect state is typically UP; other values, all of which are transient, include the following: <ul style="list-style-type: none"> <li>• DOWN ABOUT_TO_DOWN ABOUT_TO_CONNECT</li> <li>• CONNECTING</li> <li>• ABOUT_TO_RECONNECT</li> <li>• RECONNECTING</li> <li>• ABOUT_TO_RESYNC</li> <li>• RESYNCING</li> <li>• NEED_RESYNC_RETRY</li> <li>• ABOUT_TO_RESYNC_RETRY</li> <li>• RETRYING_RESYNC</li> <li>• ABOUT_TO_DISCONNECT</li> <li>• DISCONNECTING</li> </ul>

**Table 68** show xtagatm cross-connect descriptor Field Descriptions (continued)

Field	Description
Conn-type	<p>Input—Indicates an ingress endpoint where traffic is only expected to be received into the switch.</p> <p>Output—Indicates an egress endpoint, where traffic is only expected to be sent from the interface.</p> <p>Input/output—Indicates that traffic is expected to be both send and received at this endpoint.</p>
Cast-type	Indicates whether the cross-connect is multicast.
Rx service type	Quality of service type for the receive, or ingress, direction. This is MPLS QoS <n>, (MPLS Quality of Service <n>), where n is in the range from 0 to 7 for input and input/output endpoints; this will be N/A for output endpoints. (In the first release, this is either 0 or 7.)
Rx cell rate	(Guaranteed) cell rate in the receive, or ingress, direction.
Rx peak cell rate	Peak cell rate in the receive, or ingress, direction, in cells per second. This is n/a for an output endpoint.
Tx service type	Quality of service type for the transmit, or egress, direction. This is MPLS QoS <n>, (MPLS Class of Service <n>), where n is in the range from 0 to 7 for output and input/output endpoints; this will be N/A for input endpoints.
Tx cell rate	(Guaranteed) cell rate in the transmit, or egress, direction.
Tx peak cell rate	Peak cell rate in the transmit, or egress, direction, in cells per second. This is N/A for an input endpoint.

# show xtagatm vc

To display information about terminating virtual circuits (VCs) on extended Multiprotocol Label Switching (MPLS) ATM (XTagATM) interfaces, use the **show xtagatm vc** command in user EXEC or privileged EXEC mode.

**show xtagatm vc** [*vcd* [*interface*]]

## Syntax Description

<i>vcd</i>	(Optional) Virtual circuit descriptor (virtual circuit number). If you specify the <i>vcd</i> argument, information displays about all VCs with that virtual circuit descriptor (VCD). If you do not specify the <i>vcd</i> argument, a summary description of all VCs on all XTagATM interfaces displays.
<i>interface</i>	(Optional) Interface number. If you specify the <i>interface</i> and the <i>vcd</i> arguments, information displays about the specified VC on the specified interface.

## Command Modes

User EXEC  
Privileged EXEC

## Command History

Release	Modifications
12.0(5)T	This command was introduced.

## Usage Guidelines

The columns marked VCD, VPI, and VCI display information for the corresponding private VC on the control interface. The private VC connects the XTagATM VC to the external switch. It is termed private because its VPI and VCI are only used for communication between the MPLS LSC and the switch, and it is different from the VPI and VCI seen on the XTagATM interface and the corresponding switch port.

## Examples

Each connection is listed twice in the sample output from the **show xtagatm vc** command under each interface that is linked by the connection. Connections are marked as input (unidirectional traffic flow, into the interface), output (unidirectional traffic flow, away from the interface), or in/out (bidirectional).

The following is sample output from the **show xtagatm vc** command:

```
Router# show xtagatm vc

AAL / Control Interface
Interface      VCD  VPI  VCI  Type  Encapsulation  VCD  VPI  VCI  Status
XTagATM0      1    0    32   PVC   AAL5-SNAP      2    0    33  ACTIVE
XTagATM0      2    1    33   TVC   AAL5-MUX       4    0    37  ACTIVE
XTagATM0      3    1    34   TVC   AAL5-MUX       6    0    39  ACTIVE
```

[Table 69](#) describes the significant fields shown in the display.

**Table 69** *show xtagatm vc Field Descriptions*

Field	Description
VCD	Virtual circuit descriptor (virtual circuit number).
VPI	Virtual path identifier.
VCI	Virtual circuit identifier.
Control Interf. VCD	VCD for the corresponding private VC on the control interface.
Control Interf. VPI	VPI for the corresponding private VC on the control interface.
Control Interf. VCI	VCI for the corresponding private VC on the control interface.
Encapsulation	Displays the type of connection on the interface.
Status	Displays the current state of the specified ATM interface.

**Related Commands**

Command	Description
<b>show atm vc</b>	Displays information about private ATM VCs.
<b>show xtagatm cross-connect</b>	Displays information about remotely connected ATM switches.

## snmp-server community

To set up the community access string to permit access to the Simple Network Management Protocol (SNMP), use the **snmp-server community** command in global configuration mode. To remove the specified community string, use the **no** form of this command.

```
snmp-server community string [view view-name] [ro | rw] [ipv6 nacl] [access-list-number]
```

```
no snmp-server community string
```

### Syntax Description

<i>string</i>	Community string that consists of 1 to 32 alphanumeric characters and functions much like a password, permitting access to SNMP. Blank spaces are not permitted in the community string. <b>Note</b> The sign (@) is used for delimiting the context information.
<b>view</b>	(Optional) Specifies a previously defined view. The view defines the objects available to the SNMP community.
<i>view-name</i>	(Optional) Name of a previously defined view.
<b>ro</b>	(Optional) Specifies read-only access. Authorized management stations can only retrieve MIB objects.
<b>rw</b>	(Optional) Specifies read-write access. Authorized management stations can both retrieve and modify MIB objects.
<b>ipv6</b>	(Optional) Specifies a IPv6 named access list.
<i>nacl</i>	(Optional) IPv6 named access list.
<i>access-list-number</i>	(Optional) Integer from 1 to 99 that specifies a standard access list of IP addresses or a string (not to exceed 64 characters) that is the name of a standard access list of IP addresses allowed access to the SNMP agent.  Alternatively, an integer from 1300 to 1999 that specifies a list of IP addresses in the expanded range of standard access list numbers that are allowed to use the community string to gain access to the SNMP agent.

### Command Default

An SNMP community string permits read-only access to all objects.



#### Note

If the **snmp-server community** command is not used during the SNMP configuration session, the command will automatically be added to the configuration after the **snmp host** command is used. In this case, the default password (*string*) for the **snmp-server community** will be taken from the **snmp host** command.

### Command Modes

Global configuration

### Command History

Release	Modification
10.0	This command was introduced.
12.0(14)ST	This command was integrated into Cisco IOS Release 12.0(14)ST.

Release	Modification
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	The access list values were enhanced to support the expanded range of standard access list values and to support named standard access lists.
12.0(27)S	The <b>ipv6 nacl</b> keyword/argument pair was added to support assignment of IPv6 named access lists. This keyword/argument pair is not supported in Cisco IOS 12.2S releases.
12.3(14)T	The <b>ipv6 nacl</b> keyword/argument pair was integrated into Cisco IOS Release 12.3(14)T to support assignment of IPv6 named access lists. This keyword/argument pair is not supported in Cisco IOS 12.2S releases.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

### Usage Guidelines

The **no snmp-server** command disables all versions of SNMP (SNMPv1, SNMPv2C, SNMPv3).

The first **snmp-server** command that you enter enables all versions of SNMP.

To configure SNMP community strings for the MPLS LDP MIB, use the **snmp-server community** command on the host network management station (NMS).

The **snmp-server community** command can be used to specify only an IPv6 named access list, only an IPv4 access list, or both. To configure both IPv4 and IPv6 access lists, the IPv6 access list must appear first in the command statement.



#### Note

The sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using `community@VLAN_ID` (for example, `public@100`) where 100 is the VLAN number.

### Examples

The following example shows how to set the read/write community string to newstring:

```
Router(config)# snmp-server community newstring rw
```

The following example shows how to allow read-only access for all objects to members of the standard named access list lmnop that specify the comaccess community string. No other SNMP managers have access to any objects.

```
Router(config)# snmp-server community comaccess ro lmnop
```

The following example shows how to assign the string comaccess to SNMP, allow read-only access, and specify that IP access list 4 can use the community string:

```
Router(config)# snmp-server community comaccess ro 4
```

The following example shows how to assign the string manager view restricted rw to the objects in the restricted view:

```
Router(config)# snmp-server community manager view restricted rw
```

The following example shows how to remove the community comaccess:

```
Router(config)# no snmp-server community comaccess
```

The following example shows how to disable all versions of SNMP:

```
Router(config)# no snmp-server
```

The following example shows how to configure an IPv6 access list named blue and links an SNMP community string with this access list:

```
Router(config)# ipv6 access-list blue
Router(config-ipv6-acl)# permit ipv6 any any
Router(config-ipv6-acl)# exit
Router(config)# snmp-server community comaccess rw ipv6 blue
```

#### Related Commands

Command	Description
<b>access-list</b>	Configures the access list mechanism for filtering frames by protocol type or vendor code.
<b>snmp-server enable traps</b>	Enables the router to send SNMP notification messages to a designated network management workstation.
<b>snmp-server host</b>	Specifies the targeted recipient of an SNMP notification message.
<b>snmp-server view</b>	Creates or updates a view entry.

## snmp-server enable traps (MPLS)

To enable a label switch router (LSR) to send Simple Network Management Protocol (SNMP) notifications or informs to an SNMP host, use the **snmp-server enable traps** command in global configuration mode. To disable notifications or informs, use the **no** form of this command.

**snmp-server enable traps** [*notification-type*] [*notification-option*]

**no snmp-server enable traps** [*notification-type*] [*notification-option*]

<b>Syntax Description</b>	<i>notification-type</i>	<p>(Optional) Specifies the particular type of SNMP notification(s) to be enabled on the LSR. If a notification type is not specified, all SNMP notifications applicable to the LSR are enabled and sent to the SNMP host. Any one or all of the following keywords can be specified in any combination as the <i>notification-type</i> (family name) in the <b>snmp-server enable traps</b> command:</p> <ul style="list-style-type: none"> <li>• <b>bgp</b>—Sends Border Gateway Protocol (BGP) state change notifications.</li> <li>• <b>config</b>—Sends configuration notifications.</li> <li>• <b>entity</b>—Sends entity MIB modification notifications.</li> <li>• <b>envmon</b>—Sends Cisco enterprise-specific environmental monitor notifications whenever certain environmental thresholds are exceeded. <i>Notification-option</i> arguments (below) can be specified in combination with this keyword.</li> <li>• <b>frame-relay</b>—Sends Frame Relay notifications.</li> <li>• <b>hsrp</b>—Sends Hot Standby Routing Protocol (HSRP) notifications.</li> <li>• <b>isdn</b>—Sends ISDN notifications. <i>Notification-option</i> arguments (see below) can be specified in combination with this keyword.</li> <li>• <b>repeater</b>—Sends Ethernet repeater (hub) notifications. <i>Notification-option</i> arguments (see below) can be specified in combination with this keyword.</li> <li>• <b>rsvp</b>—Sends Resource Reservation Protocol (RSVP) notifications.</li> <li>• <b>rtr</b>—Sends Service Assurance Agent/Response Time Reporter (RTR) notifications.</li> <li>• <b>snmp [authentication]</b>—Sends RFC 1157 SNMP notifications. Using the <b>authentication</b> keyword produces the same effect as not using it. Both the <b>snmp-server enable traps snmp</b> and the <b>snmp-server enable traps snmp authentication</b> forms of this command globally enable the following SNMP notifications (or, if you are using the <b>no</b> form of the command, disables such notifications): <b>authenticationFailure</b>, <b>linkUp</b>, <b>linkDown</b>, and <b>warmstart</b>.</li> <li>• <b>syslog</b>—Sends system error message (Syslog) notifications. You can specify the level of messages to be sent using the <b>logging history level</b> command.</li> </ul>
---------------------------	--------------------------	--

*notification-type*  
(continued)

- **mpls ldp**—Sends notifications about status changes in LDP sessions. Note that this keyword is specified as **mpls ldp**. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword.
- **mpls traffic-eng**—Sends notifications about status changes in MPLS label distribution tunnels. This keyword is specified as **mpls traffic-eng**. This syntax, which the CLI interprets as a two-word construct, has been implemented in this manner to maintain consistency with other MPLS commands. *Notification-option* arguments (below) can be specified in combination with this keyword.

*notification-option*

(Optional) Defines the particular options associated with the specified *notification-type* that are to be enabled on the LSR.

- **envmon [voltage | shutdown | supply | fan | temperature]**

When you specify the **envmon** keyword, you can enable any one or all of the following environmental notifications in any combination: **voltage**, **shutdown**, **supply**, **fan**, or **temperature**. If you do not specify an argument with the **envmon** keyword, all types of system environmental notifications are enabled on the LSR.

- **isdn [call-information | isdn u-interface]**

When you specify the **isdn** keyword, you can use either the **call-information** argument (to enable an SNMP ISDN call information option for the ISDN MIB subsystem) or the **isdn u-interface** argument (to enable an SNMP ISDN U interface option for the ISDN U Interfaces MIB subsystem), or both. If you do not specify an argument with the **isdn** keyword, both types of isdn notifications are enabled on the LSR.

- **repeater [health | reset]**

When you specify the **repeater** keyword, you can use either the **health** argument or the **reset** argument, or both (to enable the IETF Repeater Hub MIB [RFC 1516] notification). If you do not specify an argument with the **repeater** keyword, both types of notifications are enabled on the LSR.

- **mpls ldp [session-up | session-down | pv-limit | threshold]**

When you specify the **mpls ldp** keyword, you can use any one or all of the following arguments in any combination to indicate status changes in LDP sessions: **session-up**, **session-down**, **pv-limit**, or **threshold**. If you do not specify an argument with the **mpls ldp** keyword, all four types of LDP session notifications are enabled on the LSR.

- **mpls traffic-eng [up | down | reroute]**

When you specify the **mpls traffic-eng** keyword, you can use any one or all of the following arguments in any combination to enable the sending of notifications regarding status changes in MPLS label distribution tunnels: **up**, **down**, or **reroute**. If you do not specify an argument with the **mpls traffic-eng** keyword, all three types of tunnel notifications are enabled on the LSR.

**Defaults**

If you issue this command on an LSR without specifying any *notification-type* keywords, the default behavior of the LSR is to enable all notification types controlled by the command (some notification types cannot be controlled by means of this command).

**Command Modes**

Global configuration

**Command History**

Release	Modification
11.1	This command was introduced.
11.3	The <b>snmp-server enable traps snmp authentication</b> form of this command was introduced to replace the <b>snmp-server trap-authentication</b> command.
12.0(17)ST	The <b>mpls traffic-eng</b> keyword was added to define a class or family of specific SNMP notifications for use with the <i>notification-type</i> and <i>notification-option</i> parameters of the <b>snmp-server enable traps</b> command.
12.0(21)ST	The <b>mpls ldp</b> keyword was added to define a class or family of specific SNMP notifications for use with the <i>notification-type</i> and <i>notification-option</i> parameters of the <b>snmp-server enable traps</b> command.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.

**Usage Guidelines**

To configure an LSR to send SNMP LDP notifications, you must issue at least one **snmp-server enable traps** command on the router.

To configure an LSR to send either notifications (traps) or informs to a designated network management station (NMS), you must issue the **snmp-server host** command on that device, using the keyword (**traps** or **informs**) that suits your purposes.

If you issue the **snmp-server enable traps** command without keywords, all SNMP notification types are enabled on the LSR. If you issue this command with specific keywords, only the notification types associated with those particular keywords are enabled on the LSR.

The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. You use the latter command to specify the NMS host (or hosts) targeted as the recipient(s) of the SNMP notifications generated by SNMP-enabled LSRs in the network. To enable an LSR to send such notifications, you must issue at least one **snmp-server host** command on the LSR.

**Examples**

In the following example, the router is enabled to send all notifications to the host specified as *myhost.cisco.com*. The community string is defined as *public*.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, the router is enabled to send Frame Relay and environmental monitor notifications to the host specified as *myhost.cisco.com*. The community string is defined as *public*:

```
Router(config)# snmp-server enable traps frame-relay
Router(config)# snmp-server enable traps envmon temperature
```

```
Router(config)# snmp-server host myhost.cisco.com public
```

In the following example, notifications are not sent to any host. BGP notifications are enabled for all hosts, but the only notifications enabled to be sent to a host are ISDN notifications (which are not enabled in this example).

```
Router(config)# snmp-server enable traps bgp
```

```
Router(config)# snmp-server host bob public isdn
```

In the following example, the router is enabled to send all inform requests to the host specified as *myhost.cisco.com*. The community string is defined as *public*.

```
Router(config)# snmp-server enable traps
```

```
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

In the following example, HSRP MIB notifications are sent to the host specified as *myhost.cisco.com*. The community string is defined as *public*.

```
Router(config)# snmp-server enable hsrp
```

```
Router(config)# snmp-server host myhost.cisco.com traps version 2c public hsrp
```

#### Related Commands

Command	Description
<b>snmp-server host</b>	Specifies the intended recipient of an SNMP notification (that is, the designated NMS workstation in the network).

# snmp-server enable traps mpls ldp

To enable the sending of Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) SNMP notifications, use the **snmp-server enable traps mpls ldp** command in global configuration mode. To disable the sending of MPLS LDP notifications, use the **no** form of this command.

**snmp-server enable traps mpls ldp** [session-down | session-up | pv-limit | threshold]

**no snmp-server enable traps mpls ldp** [session-down | session-up | pv-limit | threshold]

## Syntax Description

<b>session-down</b>	(Optional) Controls (enables or disables) LDP session down notifications (mplsLdpSessionDown). This message is generated when an LDP session between the router and its adjacent LDP peer is terminated.
<b>session-up</b>	(Optional) Controls (enables or disables) LDP session up notifications (mplsLdpSessionUp). This notification is generated when the router establishes an LDP session with another LDP entity (an adjacent LDP peer in the network).
<b>pv-limit</b>	(Optional) Controls (enables or disables) Path-Vector (PV) Limit notifications (mplsLdpPathVectorLimitMismatch). This notification is generated when the router establishes an LDP session with its adjacent peer LSR, but the two LSRs have dissimilar path vector limits.
<b>threshold</b>	(Optional) Controls (enables or disables) PV Limit notifications (mplsLdpFailedInitSessionThresholdExceeded). This notification is generated after eight failed attempts to establish an LDP session between the router and an LDP peer, due to any type of incompatibility between the devices.

## Defaults

The sending of SNMP notifications is disabled.

If you do not specify any of the optional keywords, all four types of LDP notifications are enabled on the LSR.

## Command Modes

Global configuration

## Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was integrated into Cisco IOS Release 12.0(30)S.

## Usage Guidelines

The MPLS LDP **pv-limit** (mplsLdpPathVectorLimitMismatch) notification provides a warning message that can be sent to the network management station (NMS) when two routers engaged in LDP operations have a dissimilar path vector limit. Cisco recommends that all LDP-enabled routers in the network be configured with the same path vector limit.

The value of the path vector limit can range from 0 to 255; a value of 0 indicates that loop detection is off; any value other than zero up to 255 indicates that loop detection is on and, in addition, specifies the maximum number of hops through which an LDP message can pass before a loop condition in the network is sensed.

The MPLS LDP **threshold** (mplsLdpFailedInitSessionThresholdExceeded) notification object provides a warning message that can be sent to a NMS when a local LSR and an adjacent LDP peer attempt to set up an LDP session between them, but fail to do so after a specified number of attempts. The default number of attempts is 8. This default value is implemented in Cisco IOS and cannot be changed using either the CLI or an SNMP agent.

In general, Cisco routers support the same features across multiple platforms. Therefore, the most likely incompatibility to occur between Cisco LSRs is a mismatch of their respective ATM VPI/VCI label ranges.

For example, if you specify a range of valid labels for an LSR that does not overlap the range of its adjacent LDP peer, the routers will try eight times to create an LDP session between themselves before the mplsLdpFailedInitSessionThresholdExceeded notification is generated.

Operationally, the LSRs whose label ranges do not overlap continue their attempt to create an LDP session between themselves after the eight retry threshold is exceeded. In such cases, the LDP threshold exceeded notification alerts the network administrator to the existence of a condition in the network that may warrant attention.

RFC 3036, *LDP Specification*, details the incompatibilities that can exist between Cisco routers and/or other vendor LSRs in an MPLS network. Among such incompatibilities, for example, are the following:

- Nonoverlapping ATM VPI/VCI ranges (as noted above) or nonoverlapping Frame-Relay DLCI ranges between LSRs attempting to set up an LDP session
- Unsupported label distribution method
- Dissimilar protocol data unit (PDU) size
- Dissimilar LDP feature support

The **snmp-server enable traps mpls ldp** command is used with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

### Examples

In the following example, LDP-specific informs are enabled and will be sent to the host myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls ldp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public mpls-ldp
```

### Related Commands

Command	Description
<b>snmp-server host</b>	Specifies whether you want the SNMP notifications sent as traps or informs, the version of SNMP to use, the security level of the notifications (for SNMPv3), and the recipient (host) of the notifications.

## snmp-server enable traps mpls traffic-eng

To enable Multiprotocol Label Switching (MPLS) traffic engineering tunnel state-change Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps mpls traffic-eng** command in global configuration mode. To disable MPLS traffic engineering tunnel state-change SNMP notifications, use the **no** form of this command.

**snmp-server enable traps mpls traffic-eng [up | down | reroute]**

**no snmp-server enable traps mpls traffic-eng [up | down | reroute]**

Syntax Description	
<b>up</b>	(Optional) Enables only mplsTunnelUp notifications { mplsTeNotifyPrefix 1 }. MplsTunnelUp notifications are sent to a network management system (NMS) when an MPLS traffic engineering tunnel is configured and the tunnel transitions from an operationally “down” state to an “up” state.
<b>down</b>	(Optional) Enables only mplsTunnelDown notifications { mplsTeNotifyPrefix 2 }. MplsTunnelDown notifications are generated and sent to the NMS when an MPLS traffic engineering tunnel transitions from an operationally “up” state to a “down” state.
<b>reroute</b>	(Optional) Controls (enables or disables) only mplsTunnelRerouted notifications { mplsTeNotifyPrefix 3 }. MplsTunnelRerouted notifications are sent to the NMS under the following conditions:  1) The signaling path of an existing MPLS traffic engineering tunnel fails for some reason and a new path option is signaled and placed into effect (that is, the tunnel is rerouted).  or  2) The signaling path of an existing MPLS traffic engineering tunnel is fully operational, but a better path option can be signaled and placed into effect (that is, the tunnel can be reoptimized). This reoptimization can be triggered by: a) a timer, b) the issuance of an <b>mpls traffic-eng reoptimize</b> command, or c) a configuration change that requires the resignaling of a tunnel.

Defaults
SNMP notifications are disabled. If this command is used without keywords, all available trap types (up, down, reroute) are enabled.

Command Modes
Global configuration

Command History	Release	Modification
	12.0(17)S	This command was introduced.
	12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
	12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

**Usage Guidelines**

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

This command controls (enables or disables) MPLS traffic engineering tunnel notifications. MPLS Tunnel StateChange notifications, when enabled, will be sent when the connection moves from an “up” to “down” state, when a connection moves from a “down” to “up” state, or when a connection is rerouted.

If you do not specify a specific argument in conjunction with this command, all three types of MPLS traffic engineering tunnel notifications will be sent.

The **snmp-server enable traps mpls traffic-eng** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

**Examples**

The following example enables the router to send MPLS notifications to the host at the address myhost.cisco.com using the community string defined as public:

```
Router(config)# snmp-server enable traps mpls traffic-eng
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

**Related Commands**

Command	Description
<b>snmp-server host</b>	Specifies the recipient of an SNMP notification operation.
<b>snmp-server trap-source</b>	Specifies the interface that an SNMP trap should originate from.

## snmp-server enable traps mpls vpn

To enable the router to send Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) specific Simple Network Management Protocol (SNMP) notifications (traps and informs), use the **snmp-server enable traps mpls vpn** command in global configuration mode. To disable MPLS VPN specific SNMP notifications, use the **no** form of this command.

```
snmp-server enable traps mpls vpn [illegal-label] [max-thresh-cleared]
[max-threshold][mid-threshold] [vrf-down] [vrf-up]
```

```
no snmp-server enable traps mpls vpn [illegal-label] [max-thresh-cleared]
[max-threshold][mid-threshold] [vrf-down] [vrf-up]
```

Syntax Description	
<b>illegal-label</b>	(Optional) Enables a notification for any illegal labels received on a VRF interface. Labels are illegal if they are outside the legal range, do not have a Label Forwarding Information Base (LFIB) entry, or do not match table IDs for the label.
<b>max-thresh-cleared</b>	(Optional) Enables a notification when the number of routes had attempted to exceed the maximum limit and then drops below the maximum number of routes. If you attempt to create a route on a VRF that already contains the maximum number of routes, the <b>mplsNumVrfRouteMaxThreshExceeded notification is sent (if enabled)</b> . When you remove routes from the VRF so that the number of routes falls below the set limit, the <b>cMplsNumVrfRouteMaxThreshCleared</b> notification is sent. You can clear all routes from the VRF by using the <b>clear ip route vrf</b> command.
<b>max-threshold</b>	(Optional) Enables a notification that a route creation attempt was unsuccessful because the maximum route limit was reached. Another notification is not sent until the number of routes falls below the maximum threshold and reaches the maximum threshold again. The max-threshold value is determined by the <b>maximum routes</b> command in VRF configuration mode.
<b>mid-threshold</b>	(Optional) Enables a notification of a warning that the number of routes created has crossed the warning threshold. This warning is sent only at the time the warning threshold is exceeded.
<b>vrf-down</b>	(Optional) Enables a notification for the removal of a VRF from an interface or the transition of an interface to the down state.
<b>vrf-up</b>	(Optional) Enables a notification for the assignment of a VPN routing/forwarding instance (VRF) to an interface that is operational or for the transition of a VRF interface to the operationally up state.

**Defaults** This command is disabled.

**Command Modes** Global configuration

**Command History**

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(30)S	This command was updated with the <b>max-thresh-cleared</b> keyword.

**Usage Guidelines**

If this command is used without any of the optional keywords, all MPLS VPN notification types are enabled.

For the **vrf-up** (mplsVrfIfUp) or **vrf-down** (mplsVrfIfDown) notifications to be issued from an ATM or Frame Relay subinterface, you must first configure the **snmp-server traps atm subif** command or the **snmp-server traps frame-relay subif** command on the subinterfaces, respectively.

The values for **mid-threshold** and **max-threshold** are set using the **maximum routes limit {warn-threshold | warning-only}** VRF configuration mode command.

The **maximum routes** command gives you two options:

- **maximum routes limit warning-only**—generates a warning message when you attempt to exceed the limit. The specified limit is not enforced.

If you use the **maximum routes limit warning-only** command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *limit* value is reached or exceeded. No max-threshold SNMP notification is generated.

- **maximum routes limit warn-threshold**—generates a warning message when the *warn-threshold* is reached. The specified limit is enforced.

If you use the **maximum routes limit warn-threshold** command with the **snmp-server enable traps mpls vpn** command, a mid-threshold SNMP notification is generated when the *warn-threshold* value is reached. A max-threshold notification is generated when the *limit* value is reached.

The notification types described above are defined in the following MIB objects of the PPVPN-MPLS-VPN-MIB:

- mplsVrfIfUp
- mplsVrfIfDown
- mplsNumVrfRouteMidThreshExceeded
- mplsNumVrfRouteMaxThreshExceeded
- mplsNumVrfSecIllegalLabelThreshExceeded

The **cMplsNumVrfRouteMaxThreshCleared** notification type is defined in the CISCO-IETF-PPVPN-MPLS-VPN-MIB.

**Examples**

In the following example, MPLS VPN trap notifications are sent to the host specified as 172.31.156.34 using the community string named public if a VRF transitions from an up or down state:

```
Router(config)# snmp-server host 172.31.156.34 traps public mpls-vpn
Router(config)# snmp-server enable traps mpls vpn vrf-up vrf-down
```

Related Commands	Command	Description
	<b>maximum routes</b>	Sets the warning threshold and route maximum for VRFs.
	<b>snmp-server enable traps atm subif</b>	Enables ATM subinterface SNMP notifications.
	<b>snmp-server enable traps frame-relay subif</b>	Enables Frame Relay subinterface SNMP notifications.
	<b>snmp-server host</b>	Specifies the recipient of SNMP notifications.

## snmp-server host

To specify the recipient of a Simple Network Management Protocol (SNMP) notification operation, use the **snmp-server host** command in global configuration mode. To remove the specified host from the configuration, use the **no** form of this command.

```
snmp-server host {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

```
no snmp-server host {hostname | ip-address} [vrf vrf-name] [traps | informs] [version {1 | 2c | 3
[auth | noauth | priv]}] community-string [udp-port port] [notification-type]
```

### Syntax Description

<i>hostname   ip-address</i>	Name, IP address, or IPv6 address of the SNMP notification host. The <i>ip-address</i> can be an IP or IPv6 address.  The SNMP notification host is typically a network management station (NMS or SNMP manager). This host is the recipient of the SNMP traps or informs.
<b>vrf</b>	(Optional) Specifies that a Virtual Private Network (VPN) routing and forwarding (VRF) instance should be used to send SNMP notifications.
<i>vrf-name</i>	(Optional) VPN VRF instance used to send SNMP notifications.
<b>traps</b>	(Optional) Specifies that notifications should be sent as traps. This is the default.
<b>informs</b>	(Optional) Specifies that notifications should be sent as informs.
<b>version</b>	(Optional) Version of the SNMP used to send the traps. The default is 1.  If you use the <b>version</b> keyword, one of the following keywords must be specified: <ul style="list-style-type: none"> <li>• <b>1</b>—SNMPv1. This option is not available with informs.</li> <li>• <b>2c</b>—SNMPv2C.</li> <li>• <b>3</b>—SNMPv3. The most secure model because it allows packet encryption with the <b>priv</b> keyword. The default is <b>noauth</b>.</li> </ul> One of the following three optional security level keywords can follow the <b>3</b> keyword: <ul style="list-style-type: none"> <li>– <b>auth</b>—Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.</li> <li>– <b>noauth</b>—Specifies that the noAuthNoPriv security level applies to this host. This is the default security level for SNMPv3.</li> <li>– <b>priv</b>—Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).</li> </ul>
<i>community-string</i>	Password-like community string is sent with the notification operation.  <b>Note</b> You can set this string using the <b>snmp-server host</b> command by itself, but Cisco recommends that you define the string using the <b>snmp-server community</b> command prior to using the <b>snmp-server host</b> command.  <b>Note</b> The sign (@) is used for delimiting the context information.

*notification-type*

Optional) Type of notification to be sent to the host. If no type is specified, all available notifications are sent. The notification type can be one or more of the following keywords:

- **bgp**—Sends Border Gateway Protocol (BGP) state change notifications.
- **calltracker**—Sends Call Tracker call-start/call-end notifications.
- **config**—Sends configuration change notifications.
- **cpu**—Sends CPU-related notifications.
- **director**—Sends DistributedDirector-related notifications.
- **dspu**—Sends downstream physical unit (DSPU) notifications.
- **eigrp**—Sends Enhanced Interior Gateway Routing Protocol (EIGRP) stuck-in-active (SIA) and neighbor authentication failure notifications.
- **entity**—Sends Entity MIB modification notifications.
- **envmon**—Sends Cisco enterprise-specific environmental monitor notifications when an environmental threshold is exceeded.
- **flash**—Sends flash media insertion and removal notifications.
- **frame-relay**—Sends Frame Relay notifications.
- **hsrp**—Sends Hot Standby Routing Protocol (HSRP) notifications.
- **iplocalpool**—Sends IP local pool notifications.
- **ipmobile**—Sends Mobile IP notifications.
- **ipsec**—Sends IP Security (IPsec) notifications.
- **isdn**—Sends ISDN notifications.
- **l2tun-pseudowire-status**—Sends pseudowire state change notifications.
- **l2tun-session**—Sends Layer 2 tunneling session notifications.
- **llc2**—Sends Logical Link Control, type 2 (LLC2) notifications.
- **memory**—Sends memory pool and memory buffer pool notifications.
- **mpls-ldp**—Sends Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) notifications indicating status changes in LDP sessions.
- **mpls-traffic-eng**—Sends MPLS traffic engineering notifications indicating changes in the status of MPLS traffic engineering tunnels.
- **mpls-vpn**—Sends MPLS VPN notifications.
- **ospf**—Sends Open Shortest Path First (OSPF) sham-link notifications.
- **pim**—Sends Protocol Independent Multicast (PIM) notifications.
- **repeater**—Sends standard repeater (hub) notifications.
- **rsrb**—Sends remote source-route bridging (RSRB) notifications.
- **rsvp**—Sends Resource Reservation Protocol (RSVP) notifications.
- **rtr**—Sends Response Time Reporter (RTR) notifications.
- **sdlc**—Sends Synchronous Data Link Control (SDLC) notifications.

- **sdllc**—Sends SDLC Logical Link Control (SDLLC) notifications.
  - **snmp**—Sends any enabled RFC 1157 SNMP linkUp, linkDown, authenticationFailure, warmStart, and coldStart notifications.
- Note** To enable RFC 2233 compliant link up/down notifications, you should use the **snmp server link trap** command.
- **srp**—Sends Spatial Reuse Protocol (SRP) notifications.
  - **stun**—Sends serial tunnel (STUN) notifications.
  - **syslog**—Sends error message notifications (Cisco Syslog MIB). Specify the level of messages to be sent with the **logging history level** command.
  - **tty**—Sends Cisco enterprise-specific notifications when a TCP connection closes.
  - **voice**—Sends SNMP poor quality of voice traps, when used with the **snmp enable peer-trap poor qov** command.
  - **vrrp**—Sends Virtual Router Redundancy Protocol (VRRP) notifications.
  - **vsimaster**—Sends Virtual Switch Interface (VSI) Master notifications.
  - **x25**—Sends X.25 event notifications.

<b>udp-port</b>	(Optional) Specifies that SNMP notifications or informs are to be sent to an NMS host.
<i>port</i>	(Optional) UDP port number of the NMS host. The default is 162.

### Command Default

This command is disabled. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs will be sent to the host.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.



### Note

If the community-string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be inserted into the configuration. The password (community-string) used for this automatic configuration of the **snmp-server community** will be the same as specified in the **snmp-server host** command. This automatic command insertion and use of passwords is the default behavior for Cisco IOS Release 12.0(3) and later releases.

### Command Modes

Global configuration

## Command History

Release	Modification
10.0	This command was introduced.
<b>Cisco IOS Release 12 Mainline/T Train</b>	
12.0(3)T	<ul style="list-style-type: none"> <li>The <b>version 3</b> [<b>auth</b>   <b>noauth</b>   <b>priv</b>] syntax was added as part of the SNMPv3 Support feature.</li> <li>The <b>hsrp</b> notification-type keyword was added.</li> <li>The <b>voice</b> notification-type keyword was added.</li> </ul>
12.1(3)T	The <b>calltracker</b> notification-type keyword was added for the Cisco AS5300 and AS5800 platforms.
12.2(2)T	<ul style="list-style-type: none"> <li>The <b>vrf</b> <i>vrf-name</i> keyword/argument combination was added.</li> <li>The <b>ipmobile</b> notification-type keyword was added.</li> <li>Support for the <b>vsimaster</b> notification-type keyword was added for the Cisco 7200 and Cisco 7500 series.</li> </ul>
12.2(4)T	<ul style="list-style-type: none"> <li>The <b>pim</b> notification-type keyword was added.</li> <li>The <b>ipsec</b> notification-type keyword was added.</li> </ul>
12.2(8)T	<ul style="list-style-type: none"> <li>The <b>mpls-traffic-eng</b> notification-type keyword was added.</li> <li>The <b>director</b> notification-type keyword was added.</li> </ul>
12.2(13)T	<ul style="list-style-type: none"> <li>The <b>srp</b> notification-type keyword was added.</li> <li>The <b>mpls-ldp</b> notification-type keyword was added.</li> </ul>
12.3(2)T	<ul style="list-style-type: none"> <li>The <b>flash</b> notification-type keyword was added.</li> <li>The <b>l2tun-session</b> notification-type keyword was added.</li> </ul>
12.3(4)T	<ul style="list-style-type: none"> <li>The <b>cpu</b> notification-type keyword was added.</li> <li>The <b>memory</b> notification-type keyword was added.</li> <li>The <b>ospf</b> notification-type keyword was added.</li> </ul>
12.3(8)T	The <b>iplocalpool</b> notification-type keyword was added for the Cisco 7200 and 7301 series routers.
12.3(11)T	The <b>vrrp</b> keyword was added.
12.3(14)T	<ul style="list-style-type: none"> <li>Support for SNMP over IPv6 transport was integrated into Cisco IOS Release 12.3(14)T. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument.</li> <li>The <b>igrp</b> notification-type keyword was added.</li> </ul>
<b>Cisco IOS Release 12.0S</b>	
12.0(17)ST	The <b>mpls-traffic-eng</b> notification-type keyword was integrated into Cisco IOS Release 12.0(17)ST.
12.0(21)ST	The <b>mpls-ldp</b> notification-type keyword was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	<ul style="list-style-type: none"> <li>All features in the Cisco IOS Release 12.0ST train were integrated into Cisco IOS Release 12.0(22)S.</li> <li>The <b>mpls-vpn</b> notification-type keyword was added.</li> </ul>
12.0(23)S	The <b>l2tun-session</b> notification-type keyword was added.
12.0(26)S	The <b>memory</b> notification-type keyword was added.

Release	Modification
12.0(27)S	<ul style="list-style-type: none"> <li>Support for SNMP over IPv6 transport was added. Either an IP or IPv6 Internet address can be specified as the <i>hostname</i> argument.</li> <li>The <b>vrf vrf-name</b> keyword argument pair was integrated into Cisco IOS Release 12.0(27)S to support multiple Lightweight Directory Protocol (LDP) contexts for VPNs.</li> </ul>
12.0(31)S	The <b>l2tun-pseudowire-status</b> notification-type keyword was added.
<b>Release 12.2S</b>	
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(25)S	<ul style="list-style-type: none"> <li>The <b>cpu</b> notification-type keyword was added.</li> <li>The <b>memory</b> notification-type keyword was added.</li> </ul>
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

### Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, a SNMP entity that receives an inform request acknowledges the message with a SNMP response protocol data unit (PDU). If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Compared to traps, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once; an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter a **snmp-server host** command, no notifications are sent. To configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host.

To enable multiple hosts, you must issue a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the **snmp-server enable** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Some notification types cannot be controlled with the **snmp-server enable** command. For example, some notification types are always enabled and others are enabled by a different command. For example, the linkUpDown notifications are controlled by the **snmp trap link-status** command. These notification types do not require an **snmp-server enable** command.

A notification-type option's availability depends on the router type and Cisco IOS software features supported on the router. For example, the **envmon** notification type is available only if the environmental monitor is part of the system. To see what notification types are available on your system, use the command `help ?` at the end of the **snmp-server host** command.

The **vrf** keyword allows you to specify the notifications being sent to a specified IP address over a specific VRF. The VRF defines a VPN membership of a customer so data is stored using the VPN.

### Regarding Notification-Type Keywords

The *notification-type* keywords used in the **snmp-server host** command do not always match the keywords used in the corresponding **snmp-server enable traps** command. For example, the notification keyword applicable to Multiprotocol Label Switching Protocol (MPLS) traffic engineering tunnels is specified as **mpls-traffic-eng** (containing two hyphens and no intervening spaces). The corresponding parameter in the **snmp-server enable traps** command is specified as **mpls-traffic-eng** (containing an intervening space and a hyphen).

This syntax difference is necessary to ensure that the command-line interface (CLI) interprets the *notification-type* keyword of the **snmp-server host** command as a unified, single-word construct, which preserves the capability of the **snmp-server host** command to accept multiple *notification-type* keywords in the command line. The **snmp-server enable traps** commands, however, often use two-word constructs to provide hierarchical configuration options and to maintain consistency with the command syntax of related commands. Table 70 maps some examples of **snmp-server enable traps** commands to the keywords used in the **snmp-server host** command.

**Table 70 Notification Keywords and Corresponding SNMP Enable Traps Commands**

SNMP Enable Traps Command	SNMP Host Command Keyword
<b>snmp-server enable traps l2tun session</b>	<b>l2tun-session</b>
<b>snmp-server enable traps mpls ldp</b>	<b>mpls-ldp</b>
<b>snmp-server enable traps mpls traffic-eng<sup>1</sup></b>	<b>mpls-traffic-eng</b>
<b>snmp-server enable traps mpls vpn</b>	<b>mpls-vpn</b>

1. See the *Cisco IOS Multiprotocol Label Switching Command Reference* for documentation of this command.

### Examples

If you want to configure a unique SNMP community string for traps but prevent SNMP polling access with this string, the configuration should include an access list. The following example shows how to name a community string comaccess and number an access list 10:

```
Router(config)# snmp-server community comaccess ro 10
Router(config)# snmp-server host 172.20.2.160 comaccess
Router(config)# access-list 10 deny any
```



#### Note

The sign (@) is used as a delimiter between the community string and the context in which it is used. For example, specific VLAN information in BRIDGE-MIB may be polled using community@VLAN\_ID (for example, public@100) where 100 is the VLAN number.

The following example shows how to send RFC 1157 SNMP traps to a host specified named myhost.cisco.com. Other traps are enabled, but only SNMP traps are sent because only **snmp** is specified in the **snmp-server host** command. The community string is defined as comaccess.

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com comaccess snmp
```

The following example shows how to send the SNMP and Cisco environmental monitor enterprise-specific traps to address 172.30.2.160 using the community string public:

```
Router(config)# snmp-server enable traps snmp
```

```
Router(config)# snmp-server enable traps envmon
Router(config)# snmp-server host 172.30.2.160 public snmp envmon
```

The following example shows how to enable the router to send all traps to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com public
```

The following example will not send traps to any host. The BGP traps are enabled for all hosts, but only the ISDN traps are enabled to be sent to a host. The community string is defined as public.

```
Router(config)# snmp-server enable traps bgp
Router(config)# snmp-server host myhost.cisco.com public isdn
```

The following example shows how to enable the router to send all inform requests to the host myhost.cisco.com using the community string public:

```
Router(config)# snmp-server enable traps
Router(config)# snmp-server host myhost.cisco.com informs version 2c public
```

The following example shows how to send HSRP MIB informs to the host specified by the name myhost.cisco.com. The community string is defined as public.

```
Router(config)# snmp-server enable traps hsrp
Router(config)# snmp-server host myhost.cisco.com informs version 2c public hsrp
```

The following example shows how to send all SNMP notifications to company.com over the VRF named trap-vrf using the community string public:

```
Router(config)# snmp-server host company.com vrf trap-vrf public
```

The following example shows how to configure an IPv6 SNMP notification server with the IPv6 address 2001:0DB8:0000:ABCD:1 using the community string public:

```
Router(config)# snmp-server host 2001:0DB8:0000:ABCD:1 version 2c public udp-port 2012
```

The following example shows how to specify VRRP as the protocol using the community string public:

```
Router(config)# snmp-server enable traps vrrp
Router(config)# snmp-server host myhost.cisco.com traps version 2c public vrrp
```

## Related Commands

Command	Description
<b>snmp-server enable peer-trap poor qov</b>	Enables poor quality of voice notifications for applicable calls associated with a specific voice dial peer.
<b>snmp-server enable traps</b>	Enables SNMP notifications (traps and informs).
<b>snmp-server informs</b>	Specifies inform request options.
<b>snmp-server link trap</b>	Enables linkUp/linkDown SNMP traps, which are compliant with RFC 2233.
<b>snmp-server trap-source</b>	Specifies the interface (and hence the corresponding IP address) from which a SNMP trap should originate.
<b>snmp-server trap-timeout</b>	Defines how often to try resending trap messages on the retransmission queue.

## tag-control-protocol vsi

To configure the use of Virtual Switch Interface (VSI) on a particular master control port, use the **tag-control-protocol vsi** command in interface configuration mode. To disable VSI, use the **no** form of this command.

```
tag-control-protocol vsi [base-vc vpi vci] [delay seconds] [id controller-id] [keepalive timeout]
  [nak [basic | extended]] [retry timeout-count] [slaves slave-count]
```

```
no tag-control-protocol vsi [base-vc vpi vci] [delay seconds] [id controller-id] [keepalive timeout]
  [nak [basic | extended]] [retry timeout-count] [slaves slave-count]
```

### Syntax Description

<b>base-vc</b> <i>vpi vci</i>	(Optional) Determines the VPI/VCI value for the channel to the first slave. The default is 0/40.  Together with the slave value, this value determines the VPI/VCI values for the channels to all of the slaves, which are as follows: <ul style="list-style-type: none"> <li>• <i>vpi/vci</i></li> <li>• <i>vpi/vci+1</i>, and so on</li> <li>• <i>vpi/vci+slave-count-1</i></li> </ul>
<b>delay</b> <i>seconds</i>	(Optional) Specifies the delay time to start a new VSI session after the system comes up or after you enter the command. If a VSI session is already running, the <b>delay</b> keyword has no effect for the current session. The delay is implemented when a new VSI session starts. The default is 0. The valid range of values is 0 to 300.
<b>id</b> <i>controller-id</i>	(Optional) Determines the value of the controller-id field present in the header of each VSI message. The default is 1.
<b>keepalive</b> <i>timeout</i>	(Optional) Determines the value of the keepalive timer (in seconds). Make sure that the keepalive timer value is greater than the value of the retry timer times the retry timer + 1. The default is 15 seconds.

<b>nak</b> [ <b>basic</b>   <b>extended</b> ]	<p>(Optional) Allows the label switch controller (LSC) to request extended negative acknowledgment (NAK) responses from the VSI slave. The extended NAK response indicates a dangling connection on the VSI slave. If the slave sends an extended NAK response code, the LSC sends a delete connection command that enables the VSI slave to delete the dangling connection.</p> <p>Use the <b>basic</b> keyword to specify the NAK 11 and NAK 12 response codes from the VSI. If you use the <b>nak basic</b> keywords, support for extended NAK is not enabled on the LSC. The interface configuration does not indicate that basic NAK support is enabled. The output of the <b>show controller vsi session</b> command does not indicate that basic NAK support is enabled.</p> <p>Use the <b>extended</b> keyword to specify extended NAK codes 51 - 54 from the VSI, which are supported in VSI protocol version 2.4. If you use the <b>nak extended</b> keywords, support for extended NAK is enabled on the LSC. The interface configuration indicates that extended NAK support is enabled. The output of the <b>show controller vsi session</b> command also indicates that extended NAK support is enabled.</p> <p><b>Note</b> Use the <b>nak extended</b> keyword only if all VSI slaves support extended NAK codes.</p>
<b>retry</b> <i>timeout-count</i>	(Optional) Determines the value of the message retry timer (in seconds) and the maximum number of retries. The default is 8 seconds and 10 retries.
<b>slaves</b> <i>slave-count</i>	(Optional) Determines the number of slaves reachable through this master control port. The default is 14 (suitable for the Cisco BPX switch).

**Defaults**

VSI is disabled.

**Command Modes**

Interface configuration

**Command History**

Release	Modification
12.0(5)T	This command was introduced.
12.2(15)T	The <b>delay</b> keyword was added.
12.3(2)T	The <b>nak</b> keyword was added.

**Usage Guidelines**

- The command is only available on interfaces that can serve as a VSI master control port. Cisco recommends that all options to the **tag-control-protocol vsi** command be entered at the same time.
- After VSI is active on the control interface (through the earlier issuance of a **tag-control-protocol vsi** command), reentering the command may cause all associated XTagATM interfaces to shut down and restart. In particular, if you reenter the **tag-control-protocol vsi** command with any of the following options, the VSI shuts down and reactivates on the control interface:
  - **id**
  - **base-vc**
  - **slaves**

The VSI remains continuously active (that is, the VSI does not shut down and then reactivate) if you reenter the **tag-control-protocol vsr** command with only one or both of the following options:

- **keepalive**
- **retry**
- **delay**

In either case, if you reenter the **tag-control-protocol vsr** command, this causes the specified options to take on the newly specified values; the other options retain their previous values. To restore default values to all the options, enter the **no tag-control-protocol** command, followed by the **tag-control-protocol vsr** command.

## Examples

The following example shows how to configure the VSI driver on the control interface:

```
Router(config)# interface atm 0/0
Router(config-if)# tag-control-protocol vsr base-vc 0 51
```

The following example enables extended NAK support:

```
Router(config-if)# tag-control-protocol vsr nak extended
```

The following example shows that extended NAK support is enabled, as shown by the bold output:

```
Router# show running-config interface atm0/0
```

```
Building configuration...
Current configuration : 113 bytes
interface ATM0/0
 no ip address
 shutdown
 label-control-protocol vsr nak extended
 no atm ilmi-keepalive
end
```

The **show controllers vsr session** command also indicates that extended NAK support is enabled, as shown by the bold output:

```
Router# show controllers vsr session
```

Interface	Session	VCD	VPI/VCI	Switch/Slave Ids	Session State
ATM0/0	0	1	0/40	0/0	UNKNOWN
ATM0/0	1	2	0/41	0/0	UNKNOWN
ATM0/0	2	3	0/42	0/0	UNKNOWN
ATM0/0	3	4	0/43	0/0	UNKNOWN
ATM0/0	4	5	0/44	0/0	UNKNOWN
ATM0/0	5	6	0/45	0/0	UNKNOWN
ATM0/0	6	7	0/46	0/0	UNKNOWN
ATM0/0	7	8	0/47	0/0	UNKNOWN
ATM0/0	8	9	0/48	0/0	UNKNOWN
ATM0/0	9	10	0/49	0/0	UNKNOWN
ATM0/0	10	11	0/50	0/0	UNKNOWN
ATM0/0	11	12	0/51	0/0	UNKNOWN
ATM0/0	12	13	0/52	0/0	UNKNOWN
ATM0/0	13	14	0/53	0/0	UNKNOWN

**Extended NAK support is enabled on LSC**

# tunnel flow egress-records

To create a NetFlow record for packets that are encapsulated by a generic routing encapsulation (GRE) tunnel when both NetFlow and Cisco Express Forwarding (CEF) are enabled, use the **tunnel flow egress-records** command in interface configuration mode. To disable NetFlow record creation, use the **no** form of this command.

**tunnel flow egress-records**

**no tunnel flow egress-records**

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

**Defaults** A NetFlow record for encapsulated packets is not created.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.2(2)T	This command was introduced.

**Usage Guidelines** When this command is enabled on a GRE tunnel with both CEF and NetFlow enabled, a NetFlow record is created for packets that are encapsulated by the tunnel.

**Examples** The following example shows how to enable NetFlow record creation:

```
Router(config-if)# tunnel flow egress-records
```

Related Commands	Command	Description
	show ip cache flow	Displays NetFlow switching statistics.

# 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**

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

**Defaults** Disabled

**Command Modes** Interface configuration

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

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

**Examples** The following example shows how to set the mode of the tunnel to MPLS traffic engineering:

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

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.

**Usage Guidelines**

The affinity determines the attributes of the links that this tunnel will use (that is, the attributes for which the tunnel has an affinity). The attribute mask determines which link attribute the router should check. If a bit in the mask is 0, 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.

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**

The following example shows how to set the affinity of the tunnel to 0x0101 mask 0x303:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<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 auto-bw

To configure a tunnel for automatic bandwidth adjustment and to control the manner in which the bandwidth for a tunnel is adjusted, use the **tunnel mpls traffic-eng auto-bw** command in interface configuration mode. To disable automatic bandwidth adjustment for a tunnel, use the **no** form of this command.

```
tunnel mpls traffic-eng auto-bw [collect-bw] [frequency seconds] [max-bw number]
[min-bw number]
```

```
no tunnel mpls traffic-eng auto-bw
```

Syntax Description	
<b>collect-bw</b>	(Optional) Collects output rate information for the tunnel, but does not adjust the tunnel's bandwidth.
<b>frequency seconds</b>	(Optional) The interval between bandwidth adjustments. The specified interval can be from 300 to 604800 seconds. Do not specify a value lower than the output rate sampling interval specified in the <b>mpls traffic-eng auto-bw</b> global configuration command.
<b>max-bw number</b>	(Optional) Maximum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.
<b>min-bw number</b>	(Optional) Minimum automatic bandwidth, in kbps, for this tunnel. The value can be from 0 to 4294967295.

### Defaults

If the command is entered with no optional keywords or arguments, automatic bandwidth adjustment for the tunnel is enabled, with adjustments made every 24 hours and with no constraints on the bandwidth adjustments made.

If the **collect-bw** keyword is entered, the tunnel's bandwidth is sampled but not adjusted, and the other keywords, if any, are ignored.

If the **collect-bw** keyword is not entered and some, but not all of the other keywords are entered, the defaults for the options not entered are: **frequency**, every 24 hours; **min-bw**, unconstrained (0); **max-bw**, unconstrained.

### Command Modes

Interface configuration

### Command History

Release	Modification
Release 12.2(4)T	This command was introduced.

### Usage Guidelines

To sample the bandwidth used by a tunnel without automatically adjusting it, specify the **collect-bw** keyword in the **tunnel mpls traffic-eng auto-bw** command.

If you enter the **tunnel mpls traffic-eng auto-bw** command without the **collect-bw** keyword, the tunnel's bandwidth is adjusted to the largest average output rate sampled for the tunnel since the last bandwidth adjustment for the tunnel was made.

To constrain the bandwidth adjustment that can be made to a tunnel, use the **max-bw** and/or **min-bw** keywords and specify the permitted maximum allowable bandwidth and/or minimum allowable bandwidth, respectively.

The **no** form of the **tunnel mpls traffic-eng auto-bw** command disables bandwidth adjustment for the tunnel and restores the configured bandwidth for the tunnel bandwidth where “configured bandwidth” is determined as follows:

- If the tunnel bandwidth was explicitly configured via the **tunnel mpls traffic-eng bandwidth** command after the running configuration was written (if at all) to the startup configuration, the “configured bandwidth” is the bandwidth specified by that command.
- Otherwise, the “configured bandwidth” is the bandwidth specified for the tunnel in the startup configuration.



**Note**

When you save the router configuration, the current bandwidth (not the originally configured bandwidth) is saved for tunnels with automatic bandwidth enabled.



**Note**

Each **tunnel mpls traffic-eng auto-bw** command supersedes the previous one. Therefore, if you want to specify multiple arguments for a tunnel, you must specify them all in a single **tunnel mpls traffic-eng auto-bw** command.



**Note**

Keywords for the **tunnel mpls traffic-eng auto-bw** command are order-dependent; you must enter them in the order in which they are listed in the command format.

**Examples**

The following example shows how to enable automatic bandwidth adjustment for tunnel102 and specify that the adjustments are to occur every hour:

```
Router(config)# interface tunnel102
Router(config-if)# tunnel mpls traffic-eng auto-bw frequency 3600
```

**Related Commands**

Command	Description
<b>mpls traffic-eng auto-bw timers</b>	Enables automatic bandwidth adjustment on a platform for tunnels configured for bandwidth adjustment.
<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.

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

**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	Command	Description
	<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**] *bandwidth*

**no tunnel mpls traffic-eng bandwidth** [**sub-pool** | **global**] *bandwidth*

## 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>bandwidth</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

Release	Modification
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.

## Usage Guidelines

Enter the bandwidth for either a global pool or subpool tunnel, not both. Only the **ip rsvp bandwidth** command specifies the two bandwidths within one command.

To set up only a global pool tunnel, leave out the keyword **sub-pool**. If you enter **global** as a keyword, the system will accept it, but 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.

## 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
	show mpls traffic-eng tunnel	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>	<b>Release</b>	<b>Modification</b>
	12.0(10)ST	This command was introduced.
12.0(29)S	The <b>bw-protect</b> keyword was added.	

<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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>mpls traffic-eng fast-reroute</b> <b>backup-prot-preemption</b>	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

# tunnel mpls traffic-eng interface down delay

To force a tunnel to go down as soon as the headend router detects that the label-switched path (LSP) is down, use the **tunnel mpls traffic-eng interface down delay** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng interface down delay** *time*

**no tunnel mpls traffic-eng interface down delay** *time*

## Syntax Description

<i>time</i>	Time, in minutes. The only valid value is 0.
-------------	--

## Defaults

There is a delay before the tunnel goes down.

## Command Modes

Interface configuration

## Command History

Release	Modification
12.0(30)S	This command was introduced.

## Usage Guidelines

You cannot specify both the **tunnel mpls traffic-eng interface down delay** command and the **tunnel mpls traffic-eng forwarding-adjacency** command. The first command that you enter would prevent the implementation of the other command and would cause the system to display error messages.

## Examples

In the following example, if the headend router detects that a link has goes down on tunnel 1000, the tunnel goes down immediately.

```
Router(config)# interface tunnel 1000
Router(config-if)# tunnel mpls traffic-eng interface down delay 0
```

# tunnel mpls traffic-eng load-share

To determine load-sharing among two or more Multiprotocol Label Switching (MPLS) traffic engineering (TE) tunnels that begin at the same router and go to an identical destination, use the **tunnel mpls traffic-eng load-share** command in interface configuration mode. To disable this feature, use the **no** form of this command.

**tunnel mpls traffic-eng load-share** *value*

**no tunnel mpls traffic-eng load-share** *value*

<b>Syntax Description</b>	<i>value</i>	A value from which the head-end router will calculate the proportion of traffic to be sent down each of the parallel tunnels. Range is between 1 and 1000000.
---------------------------	--------------	---

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

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

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.1(3)T	This command was introduced.

**Usage Guidelines** Each parallel tunnel must be configured with this command. Specify a value to indicate the *proportion* of total traffic you want to be allocated into each individual tunnel. For example, if there are to be three parallel tunnels, and you want Tunnel1 to carry half of the traffic and the other two tunnels to carry one-quarter, you should enter the following values:

- Tunnel1 -- 2
- Tunnel2 -- 1
- Tunnel3 -- 1

The ability to divide bandwidth in unequal amounts across traffic engineering tunnels has a finite granularity. This granularity varies by platform, with both hardware and software limits. If load-sharing is configured so that it exceeds the available granularity, the following message is displayed:

```
@FIB-4-UNEQUAL: Range of unequal path weightings too large for prefix x.x.x.x/y. Some available paths may not be used.
```

To eliminate this message, it is recommended that you change the requested bandwidth or load-share.

**Examples** In the following example, three tunnels are configured, with the first tunnel receiving half of the traffic and the other two tunnels receiving one-quarter:

```
interface Tunnel1
 ip unnumbered Loopback0
 no ip directed-broadcast
```

```
tunnel destination 41.41.41.41
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 2
```

```
interface Tunnel2
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 41.41.41.41
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 1
```

```
interface Tunnel3
 ip unnumbered Loopback0
 no ip directed-broadcast
 tunnel destination 41.41.41.41
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng path-option 10 dynamic
tunnel mpls traffic-eng load-share 1
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show ip route</b>	Displays routing table information about tunnels, including their traffic share.
<b>tunnel mpls traffic-eng bandwidth</b>	Configures bandwidth in Kbps for an MPLS traffic engineering tunnel.

# 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.

**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.

## 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)# tunnel mpls traffic-eng priority 1
```

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

# tunnel mpls traffic-eng record-route

To include the interface address for the label switched path (LSP) in the Record Route Object (RRO) for an RESV message, use the **tunnel mpls traffic-eng record-route** command in interface configuration mode. To remove the interface address for the LSP in the RRO for the RESV message, use the **no** form of this command.

**tunnel mpls traffic-eng record-route**

**no tunnel mpls traffic-eng record-route**

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

**Command Default** By default, this command is disabled. The interface addresses for the LSP are not included in the RRO of the RESV message. The **record-route** option is automatically enabled when the **tunnel mpls traffic-eng fast-reroute** command for the fast-reroute (FRR) feature is enabled at the headend.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(5)S	This command was introduced.
	12.0(7)T	This command was integrated into Cisco IOS Release 12.0(7)T.

**Usage Guidelines** The RRO has two functions. It records the route of the LSP that can be used in loop prevention, and it records labels that are used by FRR.

The contents of a RRO are a series of variable-length data items called subobjects.

If record route is enabled, the RRO contains details in the following order: node-ID, interface address, and label.

**Examples** The following example shows how to include the interface address using the **tunnel mpls traffic-eng record-route** command:

```
interface tunnel1
ip unnumbered loopback0
no ip direct-broadcast
tunnel destination 192.168.1.5
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng bandwidth 100
tunnel mpls traffic-eng priority 1 1
tunnel mpls traffic-eng path-option 1 dynamic
tunnel mpls traffic-eng record-route
```

Related Commands,	Command	Description
	<b>show ip rsvp reservation</b>	Displays current RSVP related receiver information in the database.
	<b>show mpls traffic-eng tunnels</b>	Displays information on the source, destination, path and interface of MPLS TE tunnels.
	<b>tunnel mpls traffic-eng fast-reroute</b>	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

# tunnel tsp-hop

To define hops in the path for the label switching tunnel, use the **tunnel tsp-hop** command in interface configuration mode. To remove these hops, use the **no** form of this command.

```
tunnel tsp-hop hop-number ip-address [lasthop]
```

```
no tunnel tsp-hop hop-number ip-address [lasthop]
```

Syntax Description		
<i>hop-number</i>		The sequence number of the hop being defined in the path. The first number is 1, which identifies the hop just after the head hop.
<i>ip-address</i>		The IP address of the input interface on that hop.
<b>lasthop</b>		(Optional) Indicates that the hop being defined is the final hop in the path (the tunnel destination).

**Defaults** No hops are defined.

**Command Modes** Interface configuration

Command History	Release	Modification
	11.1 CT	This command was introduced.

**Usage Guidelines** The list of tunnel hops must specify a strict source route for the tunnel. In other words, the router at hop <n> must be directly connected to the router at hop <n>+1.

**Examples** The following example shows how to configure a two-hop tunnel. The first hop router/switch is 172.16.0.2, and the second and last hop is router/switch 172.17.0.2.

```
Router(config)# interface tunnel 5

Router(config-if)# tunnel mode mpls traffic-eng
Router(config-if)# ip unnumbered e0/1
Router(config-if)# tunnel tsp-hop 1 172.16.0.2
Router(config-if)# tunnel tsp-hop 2 172.17.0.2 lasthop
```

Related Commands	Command	Description
	<b>tunnel mpls traffic-eng affinity</b>	Sets the encapsulation mode of the tunnel to label switching.

# vpn id

To set or update a Virtual Private Network (VPN) ID on a VPN routing/forwarding instance (VRF), use the **vpn id** command in VRF configuration mode. To remove the VPN ID from the VRF, use the **no** form of this command.

**vpn id** *oui:vpn-index*

**no vpn id** [*oui:vpn-index*]

## Syntax Description

<i>oui</i>	Organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets.
<i>vpn-index</i>	Identifies the VPN within the company. This VPN index is restricted to four octets.

## Defaults

The VPN ID is not set.

## Command Modes

VRF configuration

## Command History

Release	Modification
12.0(17)ST	This command was introduced.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.

## Usage Guidelines

Each VRF configured in a provider edge (PE) router can have a VPN ID. Use the same VPN ID for the PE routers that belong to the same VPN. Make sure the VPN ID is unique for each VPN in the service provider network.

To change the VPN ID, issue the command again. The new ID overwrites the old one.

## Examples

The following example shows how to assign the VPN ID of 0000a100003f6c to a VRF called vpn1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id a1:3f6c
```

## Related Commands

Command	Description
<b>show ip vrf detail</b>	Displays all the VRFs on a router.
<b>show ip vrf id</b>	Displays all the VPN IDs that are configured in the router and their associated VRF names and VRF route distinguishers (RDs).

## xconnect

To bind an Ethernet, 802.1q VLAN, or Frame Relay attachment circuit to a Layer 2 Tunnel Protocol Version 3 (L2TPv3) pseudowire for xconnect service and enter xconnect configuration mode, use the **xconnect** command in interface configuration mode.

```
xconnect peer-ip-address vcid pseudowire-parameters [sequencing {transmit | receive | both}]
```

Syntax Description	
<i>peer-ip-address</i>	IP address of the remote provider edge (PE) peer.
<i>vcid</i>	The 32-bit identifier of the virtual circuit between the routers at each end of the L2TPv3 control channel.
<i>pseudowire-parameters</i>	Encapsulation and pseudowire class parameters to be used for the L2TPv3 control channel. At least one of the following pseudowire parameters must be configured: <ul style="list-style-type: none"> <li>• <b>encapsulation</b> {<b>l2tpv3</b> [<b>manual</b>]   <b>mpls</b>}—The encapsulation pseudowire class parameter specifies the tunneling method used to encapsulate data in the pseudowire:               <ul style="list-style-type: none"> <li>– <b>l2tpv3</b>—L2TPv3 is the tunneling method to be used.</li> <li>– <b>manual</b>—(Optional) No signaling is to be used in the L2TPv3 control channel. This command places the router in xconnect configuration mode for manual configuration of L2TPv3 parameters for the attachment circuit.</li> <li>– <b>mpls</b>—Multiprotocol Label Switching (MPLS) is the tunneling method to be used.</li> </ul> </li> <li>• <b>pw-class</b> <i>pw-class-name</i>—The pseudowire class configuration from which the data encapsulation type (L2TPv3) will be taken. This option is mandatory if you select L2TPv3 as your data encapsulation method.</li> </ul>
<b>sequencing</b>	(Optional) Sets the sequencing method to be used for packets received or sent in L2TP sessions.
<b>transmit</b>	(Optional) Sequencing of L2TP data packets received from the L2TPv3 session.
<b>receive</b>	(Optional) Sequencing of L2TP data packets sent into the L2TPv3 session.
<b>both</b>	(Optional) Sequencing of L2TP data packets that are both sent and received from the L2TPv3 session.

**Defaults** Use L2TPv3 as the data encapsulation method with sequencing off.

**Command Modes** Interface configuration

Command History	Release	Modification
	12.0(23)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

**Usage Guidelines**

The combination of the *peer-ip-address* and *vcid* arguments must be unique on the router. Each xconnect configuration must have a unique combination of *peer-ip-address* and *vcid* configuration.

**Note**

If the remote router is a Cisco 12000 series Internet router, the *peer-ip-address* argument must specify a loopback address on that router.

The same *vcid* value that identifies the attachment circuit must be configured using the **xconnect** command on the local and remote PE router at each end of an L2TPv3 session. The virtual circuit identifier creates the binding between a pseudowire and an attachment circuit.

To manually configure the L2TP settings used in the attachment circuit, enter **encapsulation l2tpv3 manual** in the **xconnect** command. This configuration is called a static L2TPv3 session. The router is placed in xconnect configuration mode, and you can then configure the following options:

- Local and remote session identifiers (using the **l2tp id** command) for local and remote PE routers at each end of the session.
- Size of the cookie field used in the L2TPv3 headers of incoming (sent) packets from the remote PE peer router (using the **l2tp cookie local** command).
- Size of the cookie field used in the L2TPv3 headers of outgoing (received) L2TP data packets (using the **l2tp cookie remote** command).
- Interval used between sending hello keepalive messages (using the **l2tp hello** command).

If you do not enter **encapsulation l2tpv3 manual** in the **xconnect** command, the data encapsulation type for the L2TPv3 session is taken from the encapsulation type configured for the pseudowire class specified with the **pseudowire-class pw-class-name** command.

The **pw-class pw-class-name** value binds the xconnect configuration of an attachment circuit to a specific pseudowire class. In this way, the pseudowire class configuration serves as a template that contains settings used by all attachment circuits bound to it with the **xconnect** command.

**Note**

If you specify the **encapsulation l2tpv3** keyword, you must specify the **pw-class** keyword.

**Examples**

The following example configures xconnect service for an Ethernet interface by binding the Ethernet circuit to the L2TPv3 pseudowire named “123 with a remote peer 10.0.3.201. The L2TP configuration settings in the pseudowire class named “vlan-xconnect” will be used.

```
Router(config)# interface Ethernet0/0.1
Router(config-if)# xconnect 10.0.3.201 123 pw-class vlan-xconnect
```

The following example enters xconnect configuration mode and manually configures L2TPv3 parameters for the attachment circuit:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# xconnect 10.0.3.201 123 encapsulation l2tpv3 manual pw-class ether-pw
Router(config-if-xconn) l2tp id 222 111
Router(config-if-xconn) l2tp cookie local 4 54321
Router(config-if-xconn) l2tp cookie remote 4 12345
Router(config-if-xconn) l2tp hello l2tp-defaults
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>l2tp-class</b>	Configures a template of L2TP control plane configuration settings that can be inherited by different pseudowire classes.
	<b>l2tp cookie local</b>	Configures the size of the cookie field used in the L2TPv3 headers of incoming packets received from the remote PE peer router.
	<b>l2tp cookie remote</b>	Configures the size of the cookie field used in the L2TPv3 headers of outgoing packets sent from the local PE peer router.
	<b>l2tp hello</b>	Specifies the use of a hello keepalive setting contained in a specified L2TP class configuration for a static L2TPv3 session.
	<b>l2tp id</b>	Configures the identifiers used by the local and remote provider edge routers at each end of an L2TPv3 session.
	<b>pseudowire-class</b>	Configures a template of pseudowire configuration settings used by the attachment circuits transported over a pseudowire.

